理。不论是 OSI 的网络管理，还是 IETF 的网络管理，都认为现代计算机网络管理系统基本上由以下 4 个要素组成。

- 网络管理者（Network Manager）
- 网管代理（Managed Agent）
- 网络管理协议（Network Management Protocol）
- 管理信息库（Management Information Base，MIB）

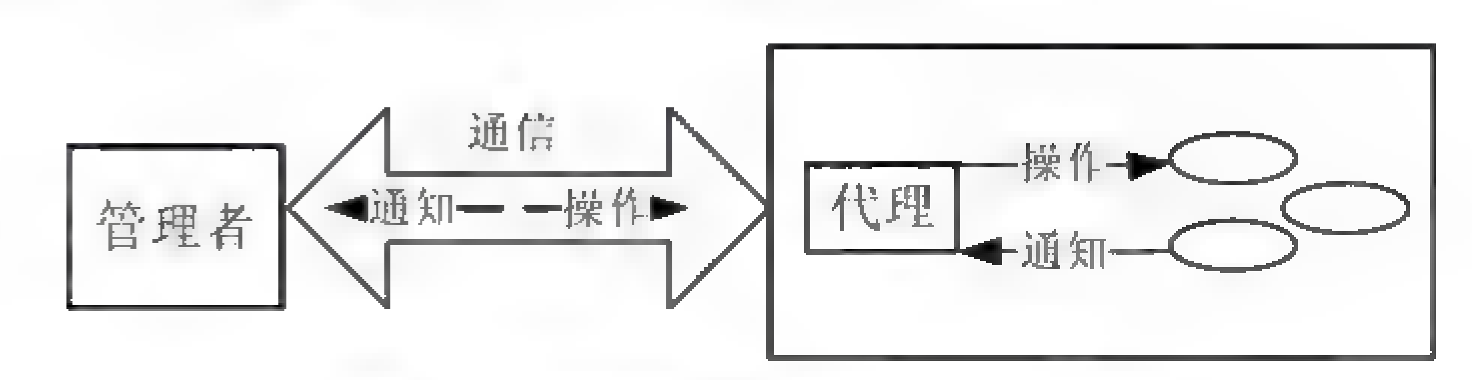


图 11-2　管理者-代理的网络管理模型

网络管理者（管理进程）是管理指令的发出者。网络管理者通过各网管代理对网络内的各种设备、设施和资源实施监视和控制。网管代理负责管理指令的执行，并且以通知的形式向网络管理者报告被管对象发生的一些重要事件。网管代理具有两个基本功能：一是从 MIB 中读取各种变量值；二是在 MIB 中修改各种变量值。MIB 是被管对象结构化组织的一种抽象。它是一个概念上的数据库，由管理对象组成，各个网管代理管理 MIB 中属于本地的管理对象，各管理网管代理控制的管理对象共同构成全网的管理信息库。

网络管理协议是最重要的部分，它定义了网络管理者与网管代理间的通信方法，规定了管理信息库的存储结构、信息库中关键词的含义以及各种事件的处理方法。在系统管理模型中，管理者角色与网管代理角色不是固定的，而是由每次通信的性质所决定。担当管理者角色的进程向担当网管代理角色的进程发出操作请求，担当网管代理角色的进程对被管对象进行操作并将被管对象发出的通报传向管理者。

11.2　简单网络管理协议

在网络管理模型中，网络管理者和代理之间需要交换大量的管理信息。这一过程必须遵循统一的通信规范，我们把这个通信规范称为网络管理协议。网络管理协议是高层网络应用协议，它建立在具体物理网络及其基础通信协议基础之上，为网络管理平台服务。

网络管理协议提供了访问任何生产厂商生产的任何网络设备，并获得一系列标准值的一致性方式。对网络设备的查询包括设备的名字、设备中软件的版本、设备中的接口数和设备中一个接口的每秒包数等。用于设置网络设备的参数包括设备的名字、网络接口的地址、网络接口的运行状态和设备的运行状态等。

目前使用的网络管理协议包括 SNMP、CMIS/CMIP、LMMP 和 RMON 等。LMMP 是 LEEE 制定的局域网和城域网管理标准，用于管理物理层和数据链路层的 OSI 设备，它利用了 CMIP。RMON 用于远程网络监视，它是 SNMP 的补充，它定义了监视局域网通信的管理信息库，与 SNMP 协议配合可以提供更有效的管理性能。下面主要介绍 SNMP 这个具有代表性的网络管理协议。

11.2.1　SNMP 概述

SNMP 是由一系列协议组和规范组成，它们提供了一种从网络上的设备中收集网络管理信息的方法。SNMP 的体系结构分为 SNMP 管理者（SNMP Manager）和 SNMP 代理者（SNMP Agent），每一个支持 SNMP 的网络设备中都包含一个网管代理，网管代理随时记录网络设备的各种信息，网络管理程序再通过 SNMP 通信协议收集网管代理所记录的信息。从被管理设备中收集数据有两种方法，一种是轮询方法，另一种是基于中断的方法。

SNMP 使用嵌入到网络设施中的代理软件来收集网络的通信信息和有关网络设备的统计数据。代理软件不断地收集统计数据，并把这些数据记录到一个管理信息库中。网管员通过向代理的 MIB 发出查询信号可以得到这些信息，这个过程就叫轮询。为了能够全面地查看一天的通信流量和变化率，管理人员必须不断地轮询 SNMP 代理，每分钟就轮询一次。这样，网管员可以使用 SNMP 来评价网络的运行状况，并分析出通信的趋势。例如，哪一个网段接近通信负载的最大能力或正在使用的通信出错等。先进的 SNMP 网管站甚至可以通过编程来自动关闭端口或采取其他矫正措施来处理历史的网络数据。

如果只是用轮询的方法，那么网络管理工作站总是在控制之下。但这种方法的缺陷在于信息的实时性，尤其是错误的实时性。多长时间轮询一次、轮询时选择什么样的设备顺序都会对轮询的结果产生影响。轮询的间隔太小，会产生太多不必要的通信量；间隔太大，而且轮询时顺序不对，那么关于一些大的灾难性事件的通知又会太慢，这就违背了积极主动的网络管理目的。与之相比，当有异常事件发生时，基于中断的方法可以立即通知网络管理工作站，实时性很强。但这种方法也有缺陷。产生错误或自陷需要系统资源，如果自陷必须转发大量的信息，那么被管理设备可能不得不消耗更多的事件和系统资源来产生自陷，这将会影响到网络管理的主要功能。

一般来说，网络管理工作站轮询在被管理设备中的代理来收集数据，并且在控制台上用数字或图形的表示方法来显示这些数据。被管理设备中的代理可以在任何时候向网络管理工作站报告错误情况，而并不需要等到管理工作站为获得这些错误情况而轮询它的时候才报告。

简单网络管理协议（SNMP）已经成为事实上的标准网络管理协议。由于 SNMP 首先是 IETF 的研究小组为了解决在因特网上的路由器管理问题提出的，因此许多人认为 SNMP 只能在 IP 上运行，但事实上，目前 SNMP 已经被设计成与协议无关的网管协议，所以它在 IP、IPX 和 AppleTalk 等协议上均可以使用。

11.2.2　SNMP 管理信息库

计算机网络管理涉及网络中的各种资源，包括两大类：硬件资源和软件资源。硬件资源是指物理介质、计算机设备和网络互连设备。物理介质通常是物理层和数据链路层设备，如网卡、双绞线和同轴电缆等；计算机设备包括处理机、打印机和存储设备及其他计算机外围设备；常用的网络互连设备有中继器、网桥、路由器和网关等。软件资源主要包括操作系统、应用软件和通信软件。通信软件是指实现通信协议的软件，例如在 FDDI、ATM 和 FR 这些主要依靠软件的网络中就大量采用了通信软件。另外，软件资源还有路由器软件和网桥软件等。

网络环境下资源的表示是网络管理的一个关键问题。目前一般采用“被管对象

（Managed Object）”来表示网络中的资源。被管对象的集合被称作 MIB，即管理信息库，所有相关的网络被管对象信息都放在其中。

> 注意：MIB 仅是一个概念上的数据库，在实际网络中并不存在一个这样的库。目前网络管理系统的实现主要依靠被管对象和 MIB，所以它们是网络管理中非常重要的概念。

MIB 是一个信息存储库，是网络管理系统中的一个非常重要的部分。MIB 定义了一种对象数据库，由系统内的许多被管对象及其属性组成。通常，网络资源被抽象为对象进行管理。对象的集合被组织为 MIB。MIB 作为设在网管代理处的管理站访问点的集合，管理站通过读取 MIB 中对象的值来进行网络监控。管理站可以在网管代理处产生动作，也可以通过修改变量值改变网管代理处的配置。

MIB 中的数据可大体分为 3 类：感测数据、结构数据和控制数据。感测数据表示测量到的网络状态。感测数据是通过网络的监测过程获得的原始信息，包括节点队列长度、重发率、链路状态和呼叫统计等。这些数据是网络的计费管理、性能管理和故障管理的基本数据；结构数据描述网络的物理和逻辑构成。对应感测数据，结构数据是静态的（变化缓慢的）网络信息，它包括网络拓扑结构、交换机和中继线的配置、数据密钥和用户记录等。这些数据是网络的配置管理和安全管理的基本数据；控制数据存储网络的操作设置。控制数据代表网络中那些可以调整参数的设置，如中继线的最大流、交换机输出链路业务分流比率和路由表等。控制数据主要用于网络的性能管理。

在现代网络管理模型中，管理信息库是网络管理系统的核心。网络操作员在管理网络时，只与 MIB 打交道，当他要对网络功能进行调整时，只须更新数据库中对应的数据即可，实际对物理网络的操作由数据库系统控制完成。现在有几种已经定义的通用的标准管理信息库，其中使用最广泛、最通用的 MIB 是 MIB-II。

11.2.3 SNMP 操作

实际的网络都是由多个厂家生产的各种设备组成的，主机可能是 SPARC 工作站或 PC，路由器可能来自于 Cisco 或者华为。要使网络管理者与不同种类的被管设备通信，就必须以一种与厂家无关的标准方式精确定义网络管理信息。SNMP 管理体系结构由管理者（管理进程）、网管代理和管理信息库（MIB）3 部分组成，该体系结构的核心是 MIB，MIB 由网管代理维护而由管理者读写。管理者是管理指令的发出者，这些指令包括一些管理操作。管理者通过各设备的网管代理对网络内的各种设备、设施和资源实施监视和控制。网管代理负责管理指令的执行，并且以通知的形式向管理者报告被管对象发生的一些重要事件。代理具有两个基本功能：从 MIB 中读取各种变量值；在 MIB 中修改各种变量值。网络中所有可管对象的集合称为 MIB，MIB 是被管对象结构化组织的一种抽象。它是一个概念上的数据库，由管理对象组成，各个代理管理 MIB 中属于本地的管理对象，各管理代理控制的管理对象共同构成全网的管理信息库。

SNMP 实体不需要在发出请求后等待响应到来，是一个异步的请求/响应协议。SNMP 仅支持对管理对象值的检索和修改等简单操作，具体讲，SNMPv1 支持 4 种操作。

① get：用于获取特定对象的值，提取指定的网络管理信息。

② get-next：通过遍历 MIB 树获取对象的值，提供扫描 MIB 树和依次检索数据的方法。

③ set：用于修改对象的值，对管理信息进行控制。

④ trap：用于通报重要事件的发生，代理使用它发送非请求性通知给一个或多个预配置的管理工作站，用于向管理者报告管理对象的状态变化。

以上 4 个操作中，前 3 个是请求由管理者发给代理，需要代理发出响应给管理者，最后一个则是由代理发给管理者，但并不需要管理者响应。

SNMP 在计算机网络应用非常广泛，虽已成为事实上的计算机网络管理的标准，但是 SNMP 还有许多自身难以克服的缺点，SNMP 不适合管理真正的大型网络，因为它是基于轮询机制的，在大型网络中效率很低；SNMP 的 MIB 模型不适合比较复杂的查询，不适合大量数据的查询；SNMP 的 trap 是无确认的，这样不能确保将那些非常严重的告警发送到管理者；SNMP 不支持如创建、删除等类型的操作，要完成这些操作，必须用 set 命令间接触发；SNMP 的安全管理较差；SNMP 定义了太多的管理对象类，管理者必须明白许多的管理对象类的准确含义。

【例 11-1】　在 Windows Server 2003 操作系统中，安装并配置 SNMP 服务。

SNMP 服务的安装方法同其他服务的安装方法类似，但是需要注意的是安装 SNMP 服务首先必须安装 TCP/IP 协议。

（1）安装 SNMP 服务

① 以管理员身份登录，在“控制面板”中选择“网络和拨号连接”并双击它，系统弹出网络和拨号连接窗口，选择菜单“高级”下的“可选网络组件”，如图 11-3 所示。

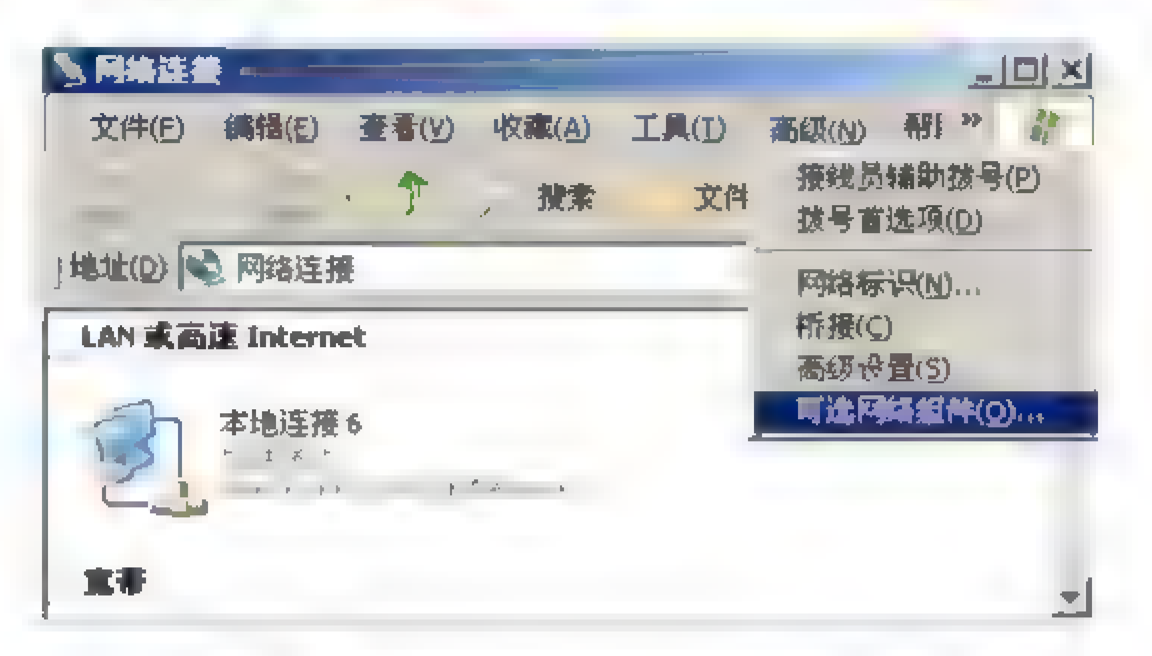


图 11-3　添加网络组件

② 系统弹出“可选网络组件向导”窗口，在“可选网络组件向导”窗口中的组件列表中选择“管理和监视工具”，如图 11-4 所示。

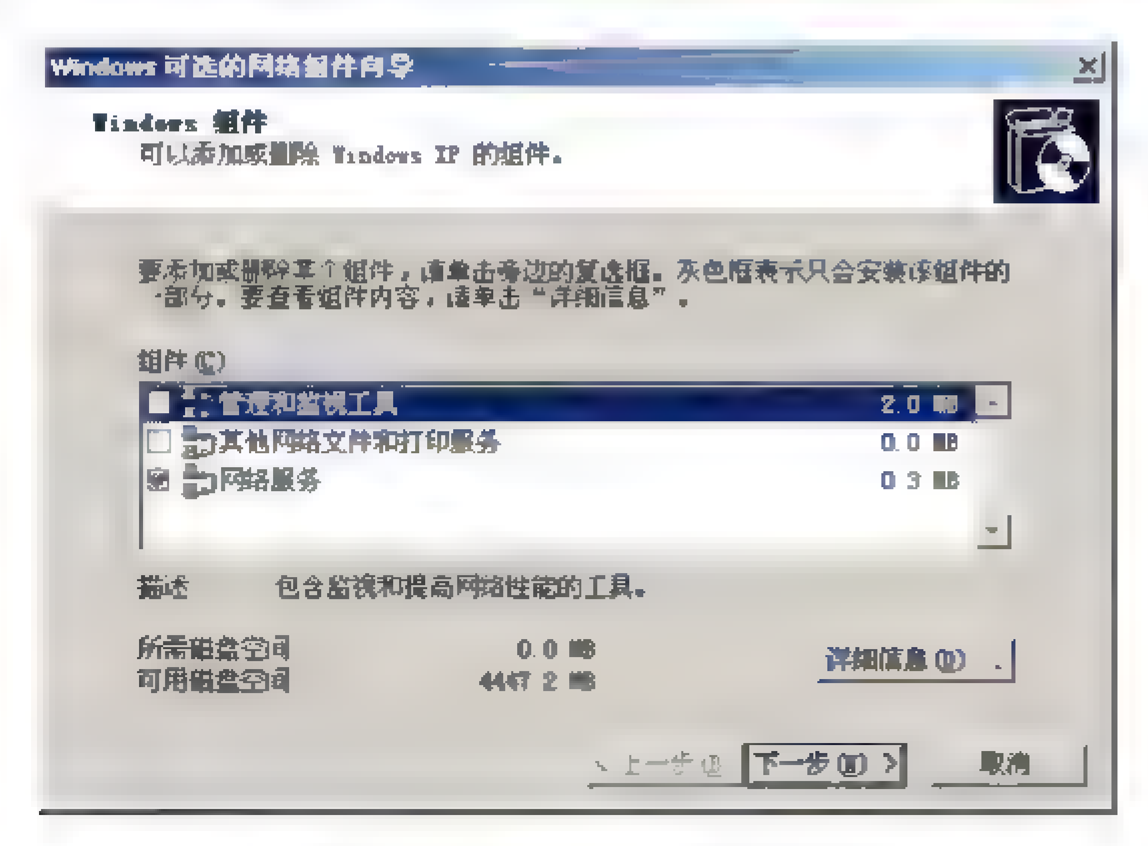


图 11-4　可选网络组件向导

③ 单击“下一步”按钮，系统提示插入系统光盘，将相应的光盘放入到CD-ROM后，单击“确定”按钮，如图11-5所示。

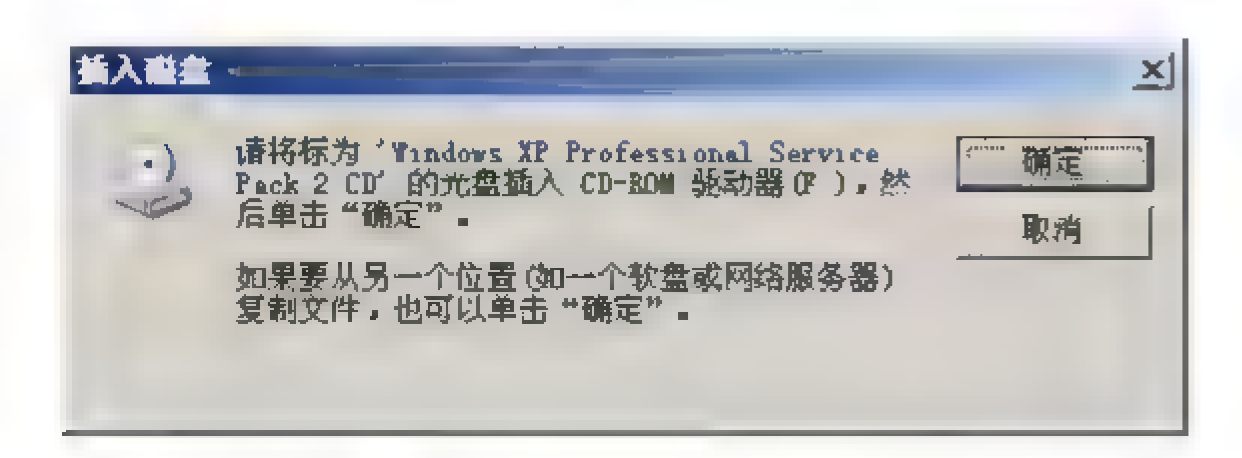


图11-5　插入系统光盘

④ 系统自动从光盘中添加SNMP服务，并完成SNMP服务的安装，如图11-6所示。

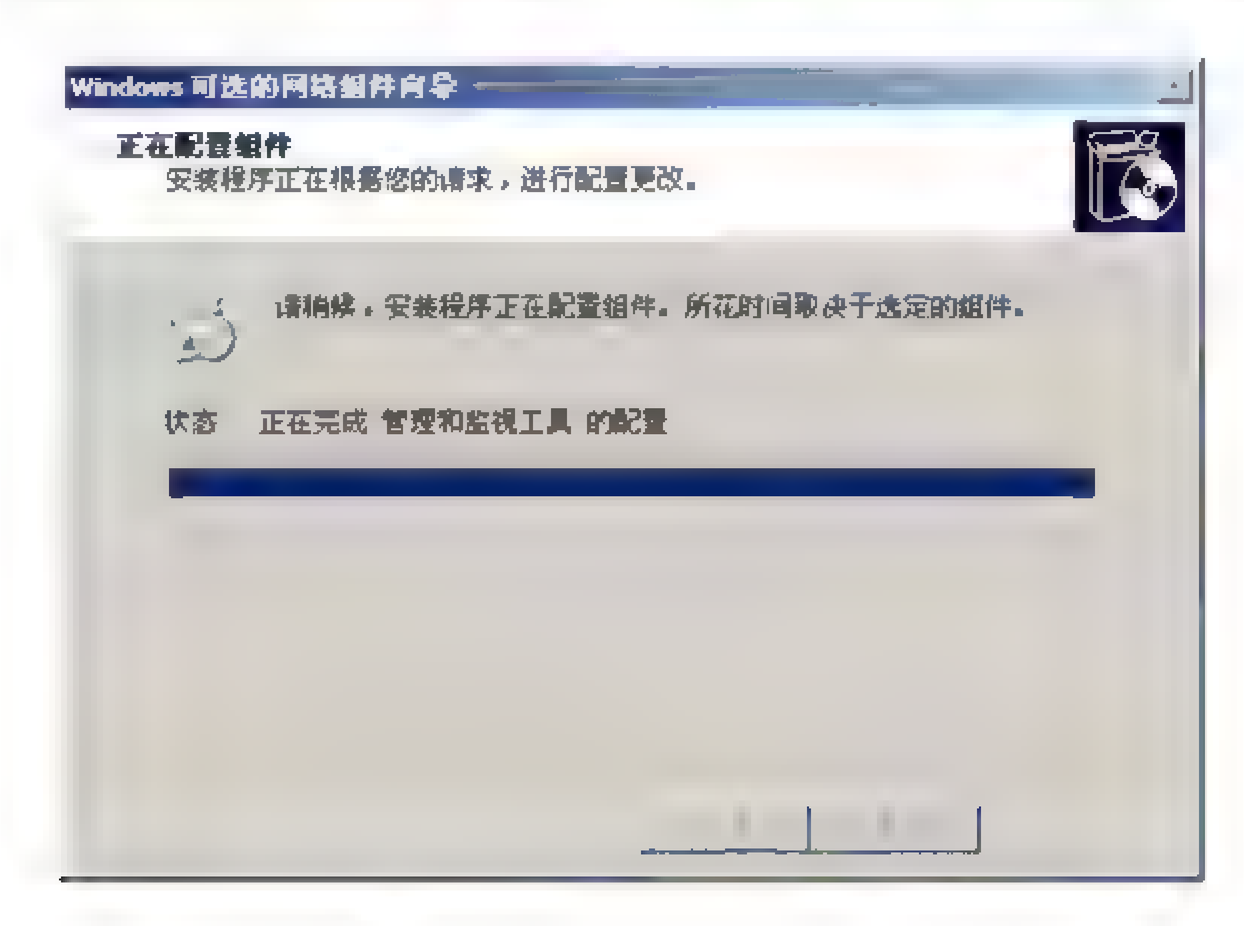


图11-6　添加SNMP服务

（2）配置SNMP服务

① 在“控制面板”中双击“管理工具”选项，弹出“管理工具”窗口，如图11-7所示。



图11-7　“管理工具”窗口

② 在控制面板中双击“服务”选项，弹出如图 11-8 所示的“服务”窗口。

图 11-8　“服务”窗口

③ 在“服务”窗口中选择 SNMP Service，并双击它，弹出“SNMP 服务属性”窗口，如图 11-9 所示。SNMP 服务使用的主要信息都在这个窗口中进行配置。

④ 选择“代理”选项卡进行代理设置，如图 11-10 所示。其中的联系人、位置和服务分别对应系统组中的 3 个对象 sysContact、sysLocation 和 sysServices。

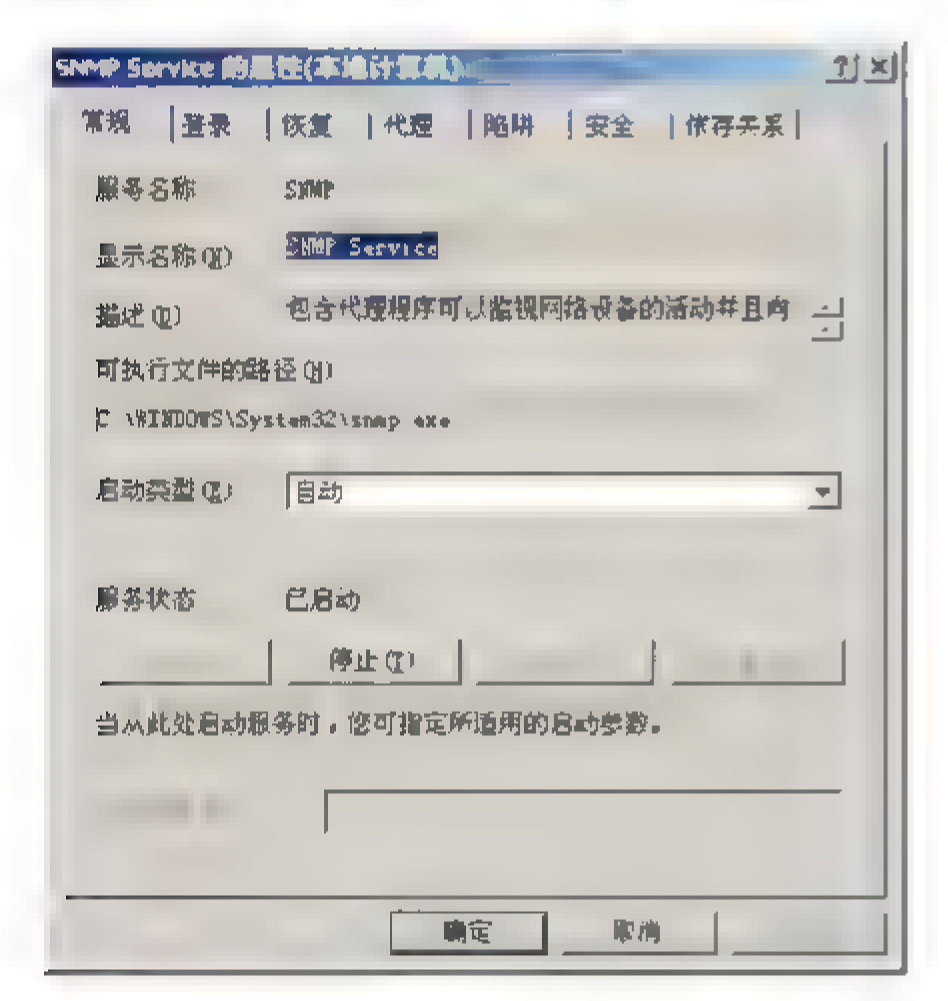


图 11-9　SNMP 属性设置

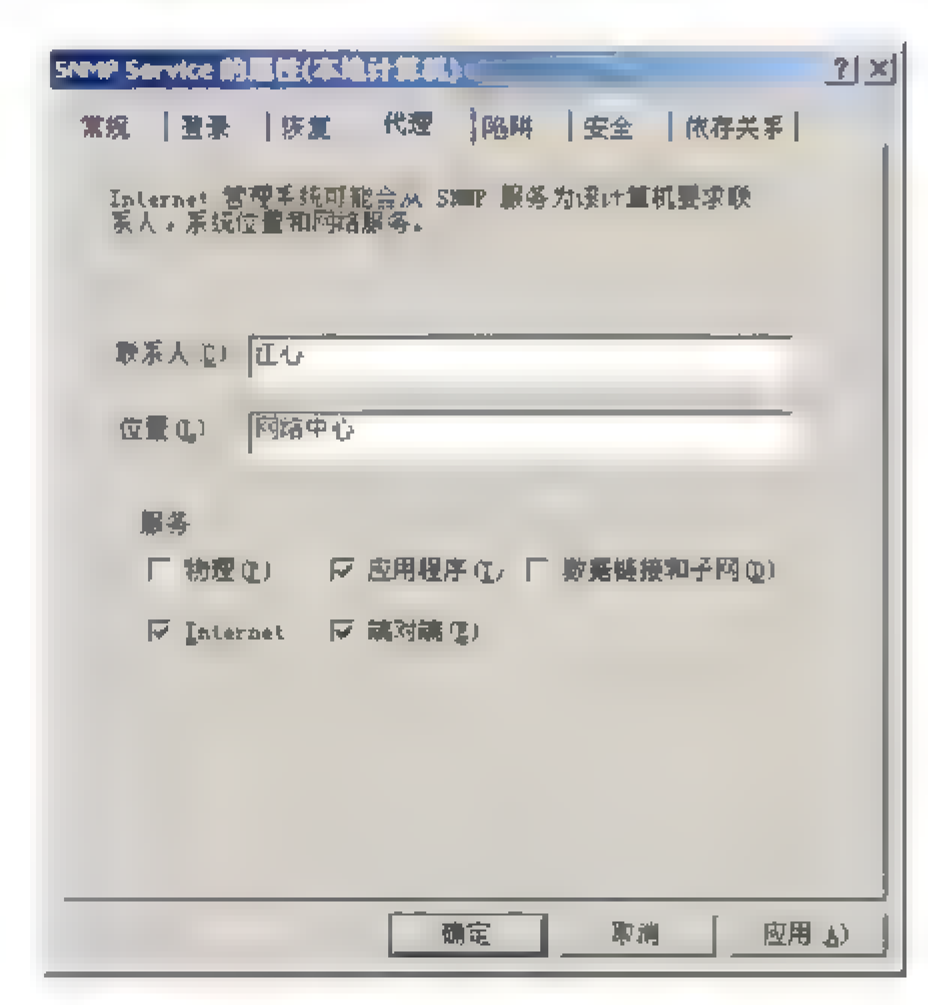


图 11-10　代理设置

⑤ 选择“陷井”选项进行陷阱配置，如图 11-11 所示。需要配置的内容包括团体名和陷井目标。起总团体名的输入要注意大小号，陷井目标可以是 IP/IPX 地址或 DNS 主机名等。

⑥ 选择“安全”选项进行安全配置，如图 11-12 所示。该部分内容是为发送需要认证的陷入报文设置的。如果不选择“发送身份认证陷阱”选项，则任何团体名都是有效的。另外可以配置代理接受任何主机或只接收特定主机的 SNMP 包，可以在该选项中进行设置。

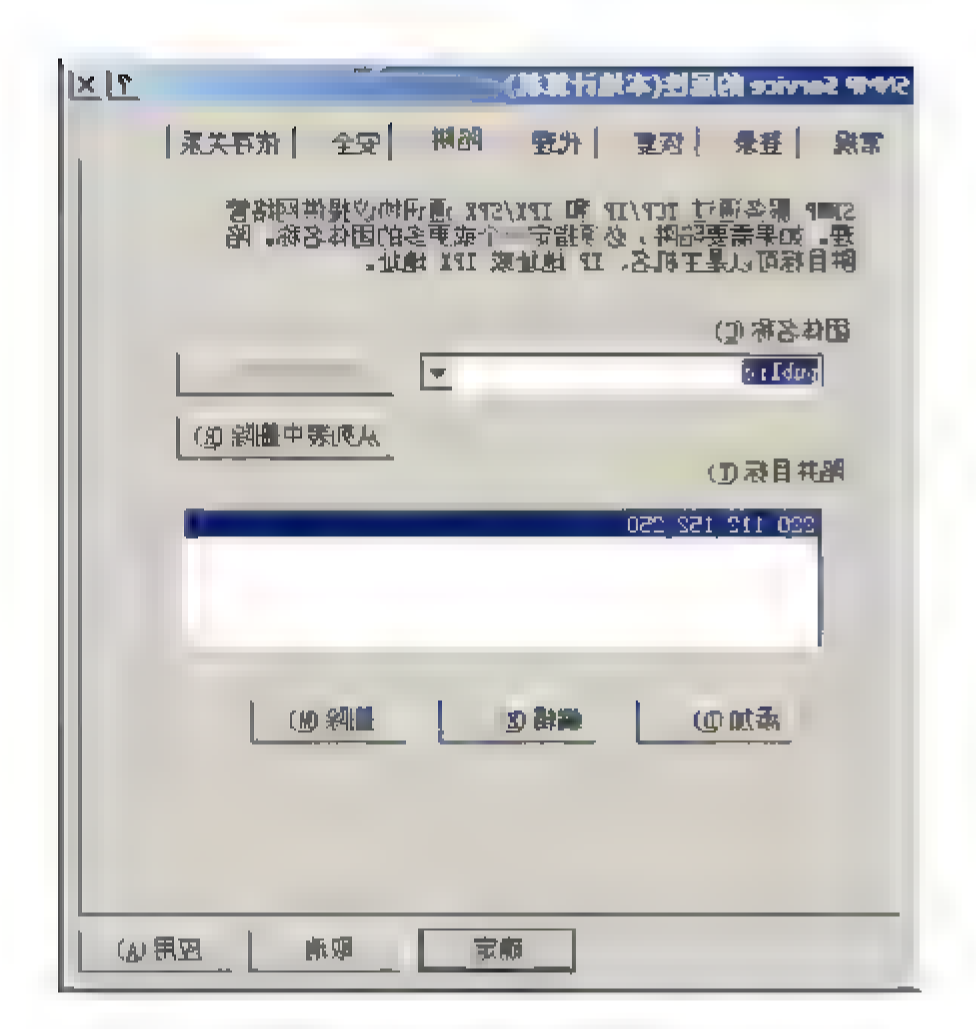




图 11-11 陷井设置

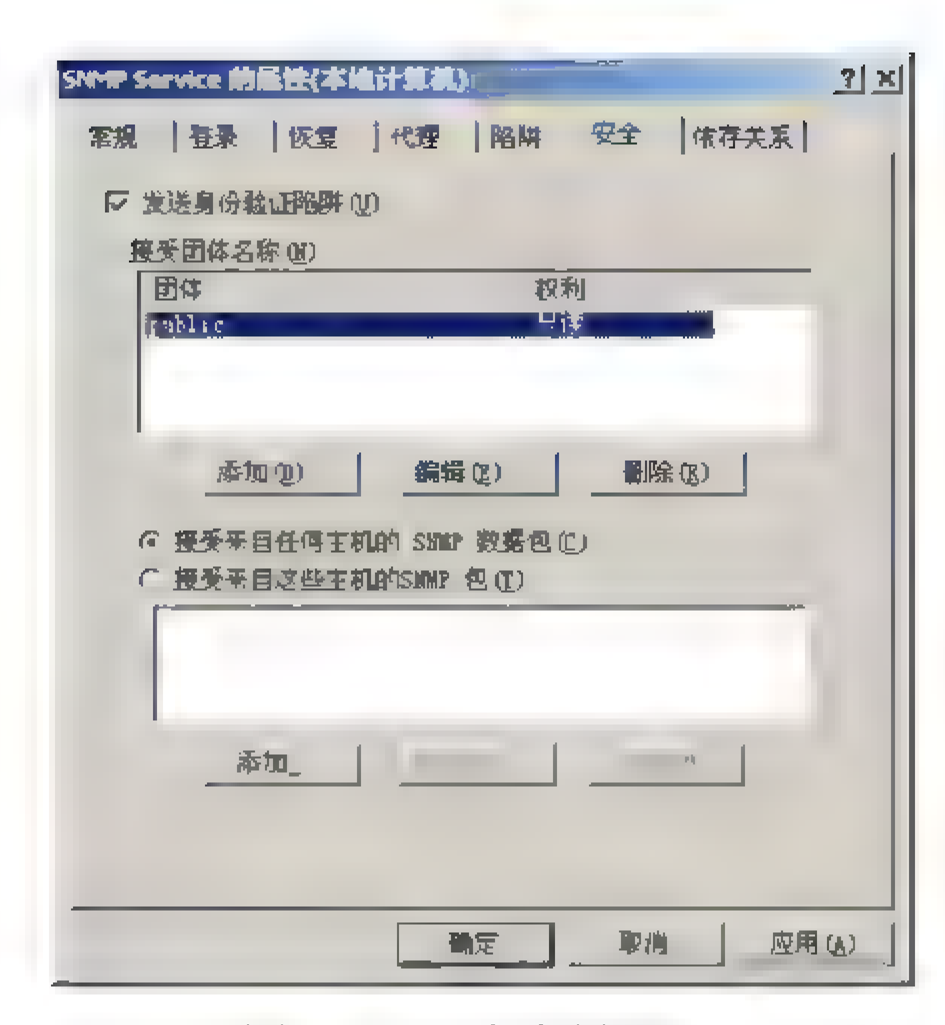


图 11-12 安全设置

⑦ 上述内容设置完成后，单击“确定”按钮，退出 SNMP 属性配置窗口，新的配置就起作用了。

（3）SNMP 服务的测试

在 SNMP 服务安装、配置完成后重新启动系统，SNMP 服务就开始工了，工作站可以接收 SNMP 的询问。在 Windows 安装盘中附带了一个 Microsoft 提供的，图形界面的测试程序 SNMPUTILG，可以用于测试 SNMP 服务，也可以测试用户开发的扩展功能。如图 11-13 所示。

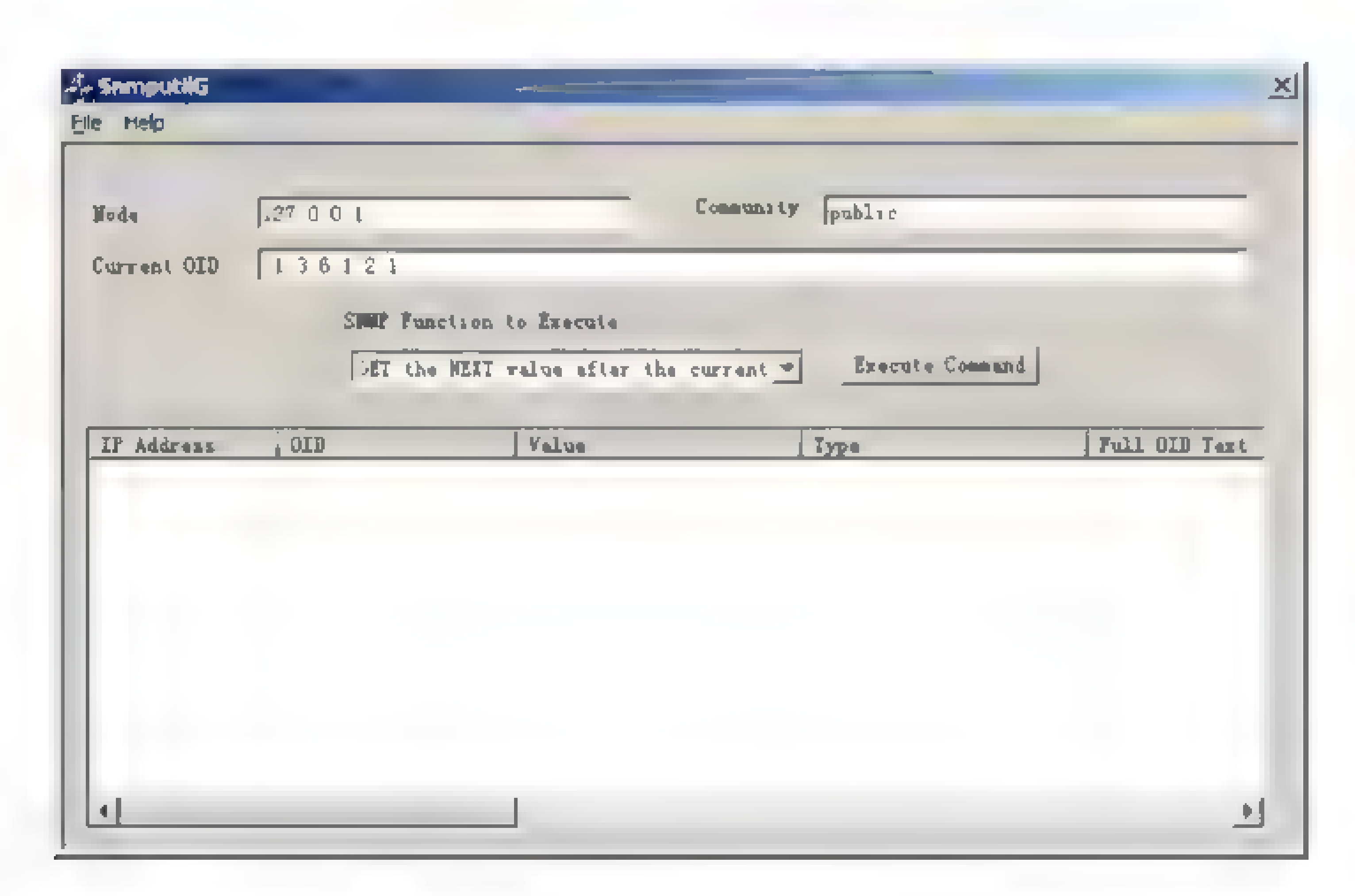


图 11-13 SNMPUTILG 程序界面

11.3 网络管理系统

通过前面的学习，明白了网络管理的概念、网络管理采用的协议以及网络管理的体系结构（管理站和代理模型）。那么网络管理的最终目标通过什么实现呢？是通过网络管理系统，也就是要通过一个实施网络管理功能的应用系统来实现。随着信息社会对网络的依赖性越来越强，网络管理系统作为附加在业务网这一棵网上的支撑系统，受到了前所未有

的重视。对于网络管理员来说，如何有效地管理网络，如何为现有网络规划设计网络管理系统（Network Management System，NMS）已变得尤为迫切。

11.3.1　网络管理系统概述

网络管理系统是用来管理网络、保障网络正常运行的软件和硬件的有机组合，是在网络管理平台的基础上实现的各种网络管理功能的集合，包括故障管理、性能管理、配置管理、安全管理和计费管理等功能。网络管理系统提供的基本功能通常包括：网络拓扑结构的自动发现、网络故障报告和处理、性能数据采集和可视化分析工具、计费数据采集和基本安全管理工具。通过网络管理系统提供的管理功能和管理工具，网络管理员就可以完成日常的各种网络管理任务了。

虽然网络管理系统是用来管理网络、保障网络正常运行的关键手段，但在实际应用中，并不能完全依赖于现成的网管产品，由于网络系统复杂多变，现成的产品往往难以解决所有的网管问题。一项权威调查显示，真正直接使用现有的成熟的商业化管理系统的单位只有少量，其余大部分是在现有的网络管理平台上二次开发的系统。也就是说一个好的网络管理系统建设是离不开自主开发的。换句话说，一个成功实用的网络管理系统建设经常伴随着在现有的网络管理平台上进行二次开发的过程。

11.3.2　HP OpenView

1. HP OpenView 简介

HP OpenView 是一个具有战略性意义的产品，它集成了网络管理和系统管理双方的优点，并把它们有机地结合在一起，形成一个单一而完整的管理系统，从而使企业在急速发展的因特网时代取得辉煌成功，立于不败之地。在 E-Services（电子化服务）的大主题下，HP OpenView 系列产品包括了统一管理平台、全面的服务和资产管理、网络安全、服务质量保障、故障自动检测和处理、设备搜索、网络存储、智能代理、因特网环境的开放式服务等丰富的功能特性。

HP 公司是最早开发网络管理产品的厂商之一。OpenView 是 HP 公司的旗舰软件产品，已成为网络管理平台的典范，有无数的第三方厂商在 OpenView 的平台上开发网络管理部门的应用。OpenView 解决方案实现了网络运作从被动无序到主动控制的过渡，使网络管理部门及时了解整个网络当前的真实情况，实现主动控制，而且 OpenView 解决方案的预防式管理工具临界值设定与趋势分析报表，可以让 IT 部门采取更具预防性的措施，以保障管理网络的健全状态。简单地说，OpenView 解决方案是从用户网络系统的关键性能入手，帮助其迅速地控制网络，然后还可以根据需要增加其他解决方案。

> 注意：HP OpenView 不是一个特定的产品，而是一个产品系列，它包括一系列管理平台，一整套网络和系统管理应用开发工具。OpenView 是管理多厂商网络设备和系统的战略平台，通过集成多厂商网络设备和系统管理产品，为用户的网络、系统、应用程序和数据库管理提供了统一的解决方案。

2. HP OpenView 管理框架

HP OpenView 解决方案框架为最终用户和应用程序开发商提供了一个基于通用管理过程的体系结构，可为用户提供集成网络、系统、应用程序和适合多用户分布式计算环境的

数据库管理。第三方的解决方案可以很容易地集成到 OpenView 系统框架众，为用户和应用开发商提供一个灵活的解决方案，以适应不断增长的、多厂商产品混杂的、分布式企业计算环境。OpenView 管理框架如图 11-14 所示。

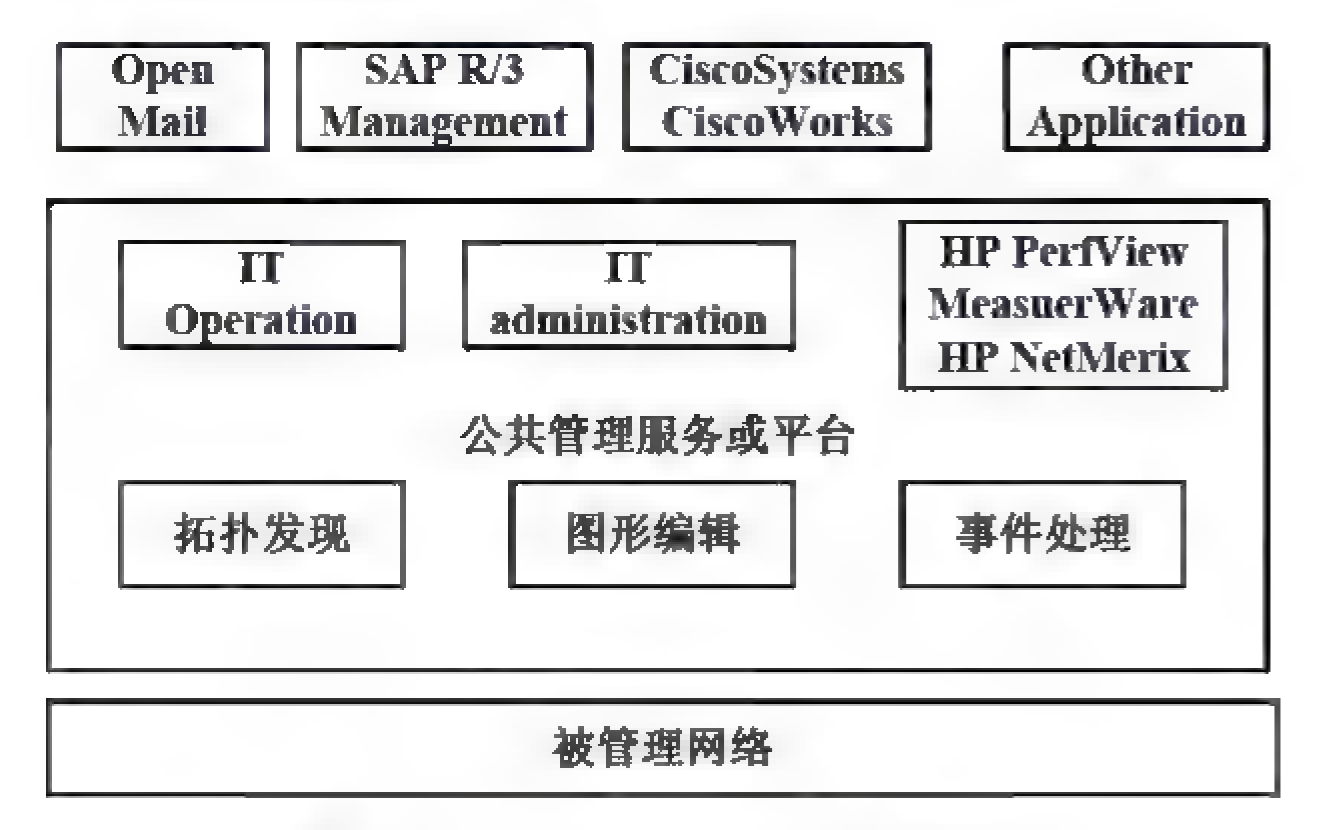


图 11-14　HP OpenView 管理框架

HP OpenView 管理框架包括以下 4 个部件。

- 用于网络管理的网络节点管理器
- 用于操作和故障管理的 IT/Operation
- 用于配置和变化管理的 IT/Administration
- 用于资源和性能管理的 HP PrefView/MeasureWare 和 HP NetMerix

3. Network Node Manager

网络对现代企业来说像"血脉"一样重要。一旦网络瘫痪，后果不堪设想。所以，企业必须主动管理网络，以便使网络能够全天候正常运作，只进行被动的网络管理是不能满足可用性要求的。同时，企业还必须管理不断变化的技术，不断适应网络的动态发展，并将各种网络环境集成在一起。HP OpenView 不但意识到了这些问题，还开发出了更强大的网络管理器（Network Node Manager，NNM）来解决这些问题。这种先进的管理解决方案能帮助企业主动管理网络环境，并不断扩展和更新基础设施。

HP OpenView 的 NNM，以其强大的功能、先进的技术和多平台适应性等特点，在全球网络范围领域得到了广泛的应用。NNM 是 HP OpenView 管理框架的基石，是第三方开发和发布网络管理应用系统的网络管理平台，也是最终用户监控和管理 TCP/IP 网络的解决方案。无论是一个小的工作组还是一个校园网，或者是一个分布式多厂商网络环境的大型企业网，NNM 都能以高度的自动化监控整个网络环境。NNM 可以通过 IP 地址、IPX 地址和 MAC 地址发现网络设备，能够运行 SNMP、HTTP 协议的网络设备或 Web 服务器。NNM 还提供了一个图形界面的 SNMP 管理应用，能够支持故障管理、配置管理和性能管理。

NNM 是 HP OpenView 家族中的主力网络管理系统软件。NNM 的分布式与监控机制，允许把处理程序就近安装于用户所处环境的本地域。通过部署多套 NNM，系统管理员就可以通过采集器与管理器管理企业的 IT 环境。采集器与管理器均可使用全版 NNM（不限管理节点数）或简版 NNM（不超过 100 个管理节点），这样一个可伸缩的解决方案可以适应不同规模网络与组织需要，可减少网络流量，从而最大限度地节约网络带宽，把带宽留给真正需要传送的商用信息。NNM 可以成功地监测和控制计算环境，它还可以提供一套有力的工具，以便管理从工作组到整个企业的分布式多厂商的网络与系统。NNM 可以用来处理

各种技术、应用以及用于建立现在或未来的、本地或全球性的网络设备。它能够为用户节省网络资产，并最大限度地利用已有资源。

11.4　网络管理技术展望

随着网络建设的初步完成，网络管理已成为当前人们关注的重点。当今的网络正在向智能化、综合化和标准化发展，同时，随着先进的计算机技术不断涌现，又给网络管理提出了新的挑战。与之相适应，网络管理技术也在不断发生新的变化，新的网络管理技术不断推广到应用中来。

11.4.1　网络管理技术的发展

尽管网络管理技术多种多样、各具特色，但是随着标准化活动的开展及系统互联的需要，网络管理发展有如下趋势。

1. 分布式网络管理

分布式网管就是设立多个域管理进程，域管理进程负责管理本域的管理对象，同时进程间进行协调和交互，以完成对全局网的管理。这样，不仅减少中央网管的负荷，而且减少了网管信息传递的时延，使管理更为有效。

当前，分布式技术主要从两个方面进行研究，一个是利用 CORBA 技术，另一个是利用移动代理技术。基于 CORBA 技术的网络管理，目前处于研究阶段；移动代理技术也仅在各个区域进行研究。何时推向市场和走进网络管理应用还是个未知数。

因此，在未来的近期使用中，可采用集中分布式的网络管理模型，具体实现管理集中、数据采集分布的管理功能，即一个管理站进行数据呈现和管理，在数据采集这种消耗大量内存和占用大量带宽方面采用分布式方法获得。实现方法为管理站具有分发代码的功能，在网络层发现网关后，同时向该网关发送代码实现该子网的各项数据采集。以此减轻管理站的负担和减少管理端网络拥塞。

2. 综合化网络管理

随着网络管理的应用性越来越突出，各种各样的网络管理系统便应运而生。这种管理系统有管理 SDH 网络的，有管理 IP 网络等等。一方面，这些网络管理系统所管理的网络存在互连或互相依赖的关系；另一方面存在多个网管系统，相互独立，分管网络的不同部分，甚至于会同时存在多个相同内容的网管系统，它们来自多个厂家，分别管理着各自的设备。这就大大增加了网络管理的复杂性。

像网络电视，它就需要管理几个方面：数字干线传输、光缆线路、前端及分前端级供电房供电、空调环境的监测维护、数据库及数据交换信息服务、前端节目源及视、音频设备和 HFC 综合接入网等。这些被管对象作为一个网管系统的被管对象是不实际的，因为不仅设备的种类不同，而且其特性大不相同，并且它们之间还有一定的关系，针对这种问题，可把它们分割为不同的网管系统，然后在高层采用一个综合的网管系统（Integrated Network Management System，INMS），以便于管理。综合网络管理系统的实现有两种方案，一种是针对已经建立起的各个专用子网的管理系统的不同情况，在此基础上建立综合网络管理系统；另一种是直接建立一个综合网络管理系统。而在我国，网络电视还没有成

熟，所以宜采用第二种方法，因此，未来的网络管理须重点向综合化发展。

3. 对业务的监控功能

传统网管都是针对网络设备的管理，并不能直接反映出设备故障对业务的影响。目前有些网管产品已经实现对进程的监控，但是有些服务，虽然服务已经终止，但是进程仍然存在，并不能明确显示对服务监控。对于客户来说，他们注重于所得到的服务，像节目的多少、节目的质量等，因此，对服务、业务的监控将是网管进一步的管理目标。

4. 安全性

安全问题是网络管理面临的主要挑战，虽然网管有 5 大功能模块，包括配置管理，但是由于网管软件多是采用 SNMP 协议（SNMPv1，SNMPv2）。安全性比较薄弱，所以基本上都没有配置功能。而最新的 SNMPv3 大大加强了安全性，因此，对 SNMPv3 的支持，也是网管软件的热点技术之一。安全性对于网络电视来说尤其重要，不仅涉及服务提供商的利益，也涉及客户的合法利益。

11.4.2 基于 Web 的网络管理

传统的网络管理系统主要着重于网络管理 3 个方面的功能，即性能管理、差错管理和配置管理。尽管这 3 个方面的功能已经涵盖了网络管理员所关注的大部分内容，但是迅速发展的企业网络已经提出了许多现有的中心网络管理软件所不能实现的要求。如网络模式从 Client/Server 到 Intranet/Web，网络远程网点和移动用户在不断增加等。

基于 Web 的网络管理（WBM）就是在这一背景下发展起来的，它的根本点在于允许通过 Web 浏览器进行网络管理。一方面它使得网络管理人员不再拘泥于固定的网络管理工作站，为管理提供了极大的灵活性；另一方面，通过 Web 浏览器来管理网络解决了多平台结构产生的互操作性问题；再有，这一管理方式提供了良好的图形界面，降低了操作的难度，进而大大降低了管理人员的培训费用。正是由于这些优点，基于 Web 的网络管理方式越来越流行。

目前，基于 Web 的网络管理主要有两种实现方式。

① 在一个内部网管工作站上运行 web 服务器，用户通过 Web 浏览器与网管工作站通信，网管工作站负责与各被管节点通信，从而间接地实现了用户和被管节点之间管理信息的交换。这个运行了 Web 服务器的工作站就是我们常说的代理。代理使用简单网络管理协议（如 TCP/IP 的 SNMP）收集被管节点的信息，代理与 Web 浏览器的通信使用 HTTP 协议。

② 将 Web 功能嵌入到网络设备中，换言之，每个网络设备都有自己的 Web 地址，网络管理员可直接通过 Web 浏览器管理这些节点。很明显，所有的管理信息都是利用 HTTP 协议传输的。

代理方式适用于大型企业，而嵌入式方式则适用于小型办公室网络环境。相比之下，代理方式保留了原有的基于管理工作站方式的所有优点，同时由于引入了基于 Web 的技术，为网络管理带来了极大的灵活性；嵌入式方式给独立的网络设备提供了图形化的管理。

11.4.3 基于 CORBA 的网络管理

1. CORBA 体系结构简介

CORBA 是 Common Object Request Broker Architecture（公共对象请求代理体系结构）

的缩写，是 OMG 定义的软件体系结构，而不是一种具体的编程语言。它定义了一套协议，符合这个协议的对象可以互相交互，不论它们是用什么样的语言写的，也不论它们运行于什么样的机器和操作系统。CORBA 体系结构如图 11-15 所示。

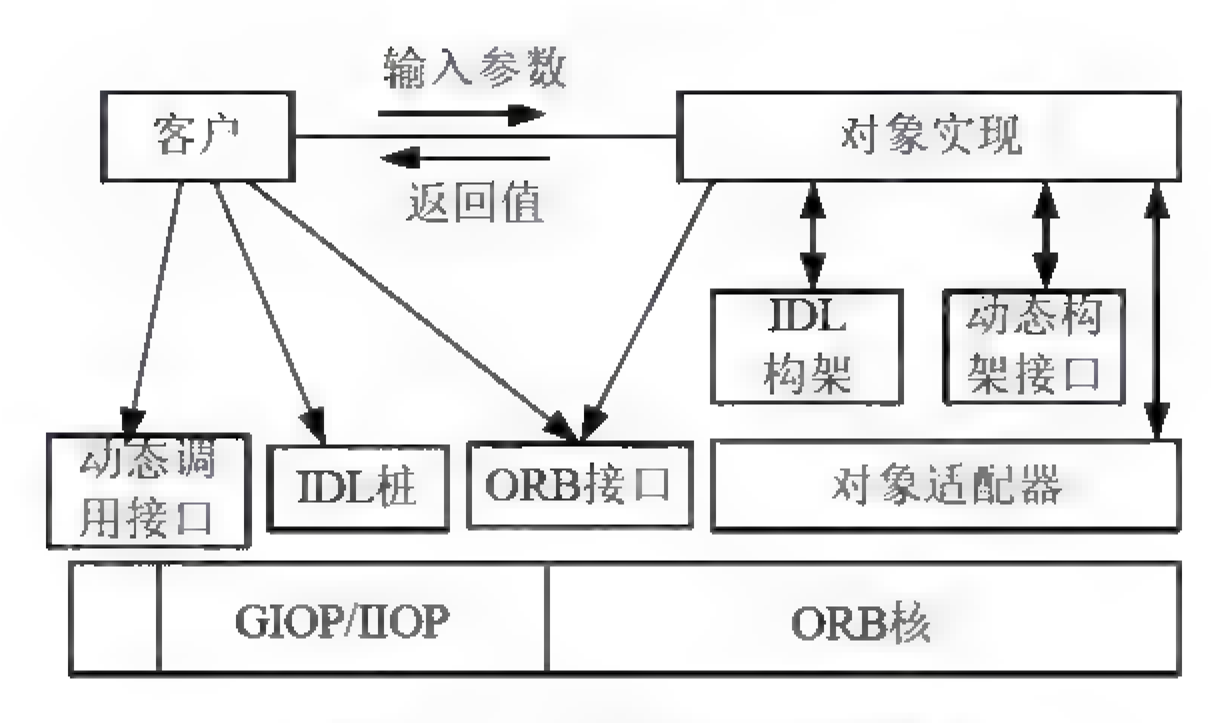


图 11-15　CORBA 体系结构

（1）接口定义语言（IDL）

OMG IDL 是描述客户对象的调用接口和对象实现接口的一种语言，用规定的语法完整定义了服务接口。IDL 是一种纯描述语言，不具有可执行性，因此不论对象实现（Object Implementation）采用何种语言，采用何种平台，分布于系统的哪个位置，客户只要知道 IDL 就可以与对象实现进行交互。IDL 编译器将 IDL 文件编译成对应编程语言的程序和桩构架程序，实现对具体编程语言的映射。

（2）对象请求代理（ORB）

ORB 是 CORBA 的核心，为客户方寻找对应的服务方，并管理服务方与客户方之间的连接，是对象之间建立客户/服务器关系的中间层，作用类似于对象总线。通过 ORB，客户可以透明地调用在某个服务对象上的方法，服务对象同该客户既可以在同一台机器上，也可以通过网络连接。

（3）对象适配器（OA）

OA 介于 ORB 和对象实现之间，代表服务器对象接受服务请求，为实例化服务器对象传递请求，制定对象标识，提供运行环境。其工作包括产生和解释对象引用、方法的调用、交互的安全性、对象实现的调用和撤销、将引用映射成对象实现和对象实现的注册等。

（4）桩程序和构架程序

客户方的桩程序负责把用户的请求进行编码，发送到对象实现端，并对接收到的处理结果进行解码，将结果返回给用户。服务方的构架程序对用户请求进行解码，定位所要求的对象方法并执行，将执行结果或异常信息编码后送回用户。

（5）ORB 间的互操作

CORBA2.0 增加了 ORB 系统间互操作规范，定义了通用 ORB 间通信协议（GIOP），详细规定了数据编码格式、传输消息格式和对传输协议的要求，提供了 GIOP 到 TCP/IP 协议的映射（IIOP），支持互联网上不同 ORB 产品间的互操作，可实现 Internet/Intranet 网络环境下基于 Web 的应用操作。

2. CORBA 网络管理的特点

CORBA 规范所遵循的面向对象的设计思想和实现方法能够贯穿网络管理系统从设计、实现、仿真、应用和维护整个生命周期，从而使得网络管理系统具有更强的可扩展、可重

用性，方便于系统升级改造。CORBA 规范实现了用户与服务器的完全分离，使得基于CORBA 规范开发的管理代理与管理器之间只要遵从相同的调用接口就可以实现开发平台的透明性、操作系统的透明性、编程语言的透明性及运行状态的透明性，这对于支持异构环境的计算机网络管理系统实现有着极大的吸引力。

CORBA 技术的使用可以使计算机网络管理和计算机系统/服务的管理基于相同的支持平台开发，方便两者的集成。

3. 基于 CORBA 的综合网络管理体系结构

在基于 CORBA 的综合网络管理系统中，CORBA 服务在网络管理系统和被管理系统之间是作为中间件，整个 INMS 以 CORBA 体系结构为基础。CORBA 可以保证 INMS 跨多个网络管理平台，重复使用子系统的被管理对象的类，而且可以集成不同的网络管理协议。因此，综合网络管理系统是一个十分庞大的处理系统，它除了要与网络设备打交道以外，还要处理本地用户和远地用户发来的网络管理的有关命令，同时还要和数据库进行交互。图 11-16 所示为基于 CORBA 的综合网络管理系统结构图。

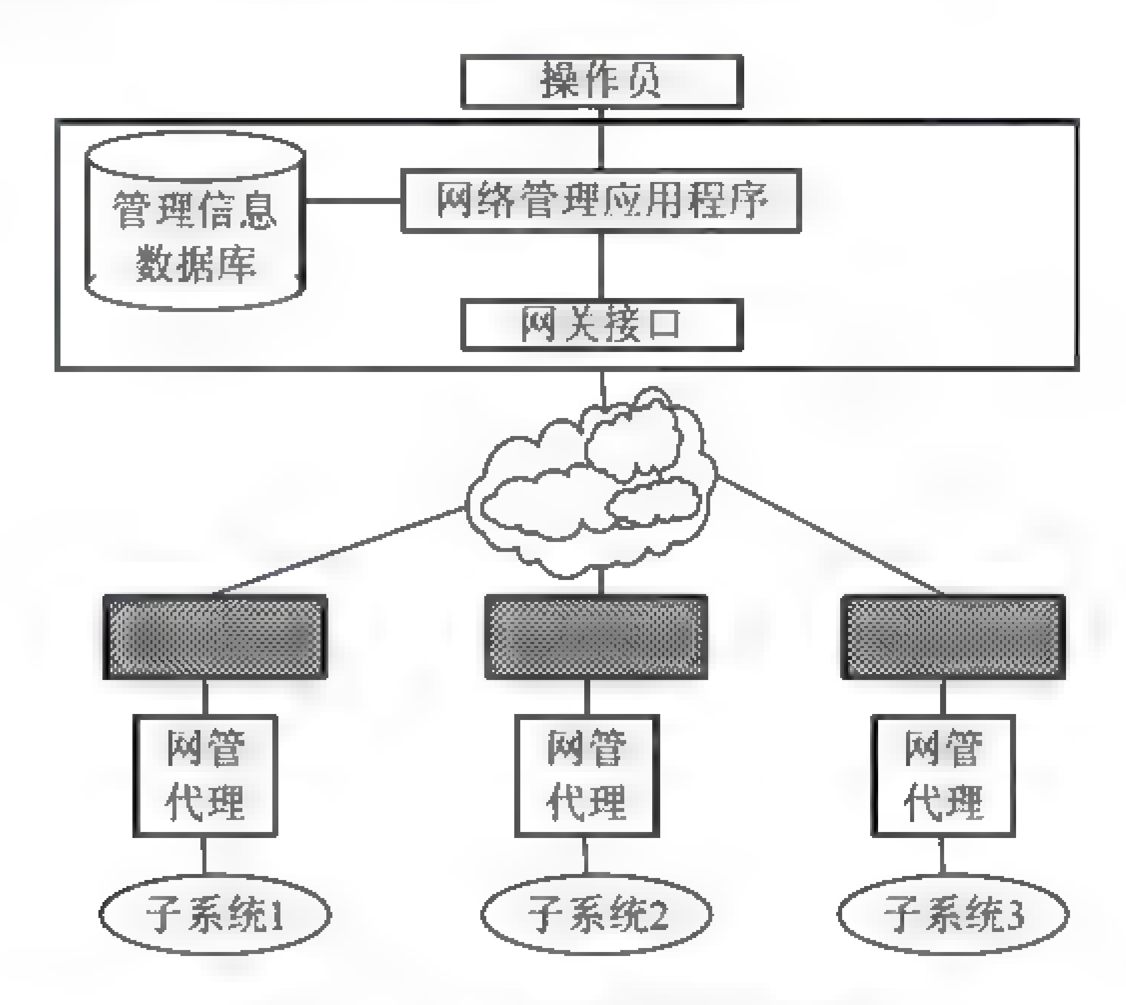


图 11-16 综合网络管理系统结构

网络管理应用程序模块是根据网络管理不同功能的需要为用户提供不同应用。网络管理应用程序模块中分性能管理、配置管理、故障管理和安全管理模块。操作员发来操作命令，将这些命令根据命令的具体格式分解成以上的用户命令向下发送，同时根据需要访问数据库，从数据库中得到一些相关的数据。

网关接口模块是根据上层用户程序发来的命令转换成符合 SNMP，CMIP 原语的形式，向下层发送相应的原语命令，并将返回的结果通过网络管理应用程序送到数据库中。它是根据 API 来进行编程实现的，通过这些 API 和网络设备进行交互。管理信息数据库模块是用来存储 MIB 库以及性能管理、配置管理、故障管理和安全管理的数据信息。

在现代通信网中，设备管理系统的软、硬件具有明显的分布式和异构性，而 CORBA 对系统的软、硬件平台不能提供良好的支持，因此能很好地适应这种情况。而且，CORBA 屏蔽了底层通信的细节，使开发人员可以着重于应用层软件的设计和开发。对已经实现的非 CORBA 网络管理系统，只要对其进行对象抽象建模，即可应用于 CORBA 系统，大大提高了代码的重用率。因此，CORBA 技术为实现综合网络管理提供了科学、高效的实现手段，它在综合网络管理系统中已得到广泛的应用。

11.4.4　基于主动网的网络管理

1. 主动网络的概念

主动网络（Active Network）是美国国防部高级研究计划署（DARPA）于 1994 年—1995 年在关于未来网络系统发展方向的讨论中提出的。主动网概念的提出是为解决网络技术快速发展所带来的问题。例如新的技术和标准在现有网络部署中，需漫长的标准化过程，无法满足新业务快速变化和涌现的需求；分层协议的冗余带来的性能低效，以致现有网络难以引入新型的网络服务；网络服务缺乏定制能力等等。

主动网络中传输的分组不仅可以携带用户的数据，而且可以携带用户定制的一段程序代码，使得分组在经过网络节点转发处理时，不仅识别头部标识，而且可以通过运行分组携带的代码，来修改、存储或重定向网络中的数据流，为分组的转发或分组的进一步处理提出建议。从而，将传统网络中“存储-转发”的处理模式改变为“存储-计算-转发”的处理模式。由于主动网增加网络中间节点（路由器或交换机）的计算能力和可编程能力，使得网络能够根据应用和用户需要定制分组转发的行为。

2. 主动网络管理

为了适应主动网络的特点，主动网络的管理模式应能突破传统网络的非对称管理模式，使网络控制与管理工作站及主动节点之间达到一种对等的关系，从而克服传统网络管理中管理端出现的瓶颈问题，也便于业务的动态加载和动态 MIB 的管理与维护。基于主动网络的管理技术是将主动网络与网络管理相结合的新型网络管理技术，势必将加大网络管理的现代化进程。主动网络管理结构如图 11-17 所示。

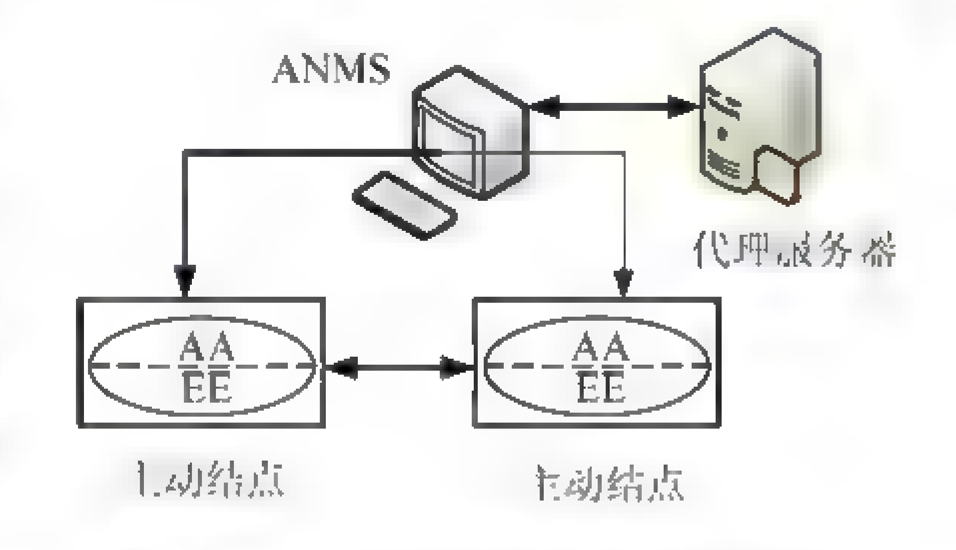


图 11-17　主动网络管理的系统结构

在主动网络管理 ANM 系统中，主动节点是主动网管所要管理的主动对象。主动节点与控制管理站（ANMS）之间的通信是一种对等的关系，而不像 SNMP 中客户端与服务端之间的非对等关系。主动节点是网管系统的主要管理对象，负责处理主动信包；执行环境（EE）提供了主动管理信包运行和处理所必需的环境；主动应用（AA）则执行主动管理信包中的代码。当管理节点需要执行某个管理任务时，它首先启动相应的管理程序，该管理程序创建一封装体报文，然后将它注入到网络中。封装体报文到达主动网络中的节点时，节点根据管理节点发出和管理程序中的策略和计算规则执行相应的程序，并根据程序决定下面的动作，通过调用节点操作系统 OS 来访问各种资源来实施网络配置管理、性能管理和故障管理等功能。

主动网络是针对传统网络中新服务实施的困难提出的，它增加了网络的计算能力，在网络的中间节点提供面向用户的编程接口，用户可以通过编程指定节点对数据的处理。这种计算是基于用户或特定应用的，从而使用户能够定制自己的服务，能够对现有各种新型应用提供灵活有效的支持，加速了新网络协议和用户服务在网络中实施和推广的进程。

11.4.5　智能化的网络管理

1. 性能管理、故障管理智能化

智能化实现主要是通过应用专家系统的方法，建立知识库和推理机。

采集数据监听管理设备的运行情况，收集管理数据，即时管理数据记录一些重要设备的关键性管理指标，如路由器、交换机的各端口的输出和输入的错误率，IP、ICMP 和 UDP 等包接收数据、发送数据，IP、ICMP 和 UDP 等包丢失率。

知识库包括事件名称、事件类型、事件特征和处理方法等，其中事件类型按设备分为接入设备、线路、实时和统计几类；事件特征包括以下性能指标。

① 路由器性能指标：端 E1 流量、CPU 利用率、内存量。

② 线路性能指标：线路流量、利用率。

③ 实时性能指标：流量、丢包率、延迟、CPU 利用率、内存余量。

④ 统计分析指标：各性能指标按不同时间段的统计数据。

知识的主要来源有两种，利用数据挖掘方法对即时管理数据库中的数据进行查找，利用知识发现，查找出其中一些规律的现象，添加入知识库；另一种是管理员自己使用利用实际经验将事件和现象归纳成事件条件和相应性能值，具体如下。

- 静态知识：根据性能指标的标准，如根据有些指标的上下阈值，并将这些翻译成知识库的事件现象条件，每种现象可能对应一个或几个事件。
- 动态知识：通过数据挖掘，查找一个规律性的现象，由此形成管理知识放入知识库中。
- 经验：根据实际经验，网络管理员可以增加一些具有规律性的现象和相应有效的处理方法。

推理机根据已监测收集到的管理数据或管理员的管理请求，利用知识库，综合分析找出网络已出现的故障，通过前项推理和后项推理对网络状态进行预测和网络故障进行诊断预测，结合网络拓扑图和网络配置表，定位故障位置，并给出处理故障的参考方案。系统给出诊断报告，对一些可以处理的故障，系统自动执行，可以立即报警或发邮件、写入日志文件等方式通知管理员。利用知识库对性能指标进行评估，可以用图形界面显示或通过邮件发给管理员性能评估报告。

2. 配置管理智能化

IP 地址的分配是一个十分烦琐的工作，随着网络规范的扩大，如何避免地址冲突将更加困难。但如果将数据库管理的方法引入到 IP 地址的分配上，则可以很好地解决这个问题。

（1）IP 地址自动分配管理

分配、查询和修改首先建立一个单位 IP 地址的总体分配表，通过这个表确定什么部门或办公地点分配什么相应的网段。另外通过一张表记录已分配地址和未分配的地址。这样通过输入新用户的部门名称或办公地点，系统可以自动分配一个未被占用的 IP 地址。同对任一已用的 IP 地址，可以迅速找出用户所属部门和办公地点。当用户改变办公地点或离职而不需要 IP 地址，系统可收回不要的 IP 地址，并重分配新的 IP 地址。

（2）IP 身份认证和授权与控制

在局域网上经常出现用户非法操作，如 IP 地址的盗用，用户在网络上非法操作等，给管理带来不必要的麻烦。而这些问题的根源是没有一个对 IP 地址的合法性的有效控制。为了实现对 IP 地址合法性的控制，可以将 IP 地址与用户信息绑定，如 MAC 地址、用户名等，可在已用 IP 地址表上加上绑定信息。

- SNMP 信息（IP、MAC 地址、端口号、端口状况和设备类型等）

- 辅助信息（工作地点、用户名、系、电话号码）
- 授权控制（操作和权限）

这样可以实时对用户身份的合法性进行检查，同时对用户在网上的操作进行监控。

用户登录时必须通过身份验证，只有通过了身份验证才有权上网，否则将不能上网。之后，不同 IP 可能权限不同，对一些重要信息可以加一些权限控制，实现自动对用户的网络使用灵活授权与控制。

3. 计费管理

对网络资源使用情况进行计账，自动监视网络流量异常的情况。因为病毒或黑客的攻击，常出现设备某端口或 PC 上的流量特别大，严重的甚至造成整个网络瘫痪。有效监视网络流量，根据标准知识库发现异常情况，自动报警，可帮助管理员快速准确地找出问题。结合前面提到的专家系统，可以给出问题和相应的解决方案。

通过建立策略库和网络资源的历史记录库，对网络信息进行不同的收费，如不同段，不同人员不同信息，如国内与国外信息不同，上网高峰时与平时不同，来调节网络的拥挤和阻塞。利用 IP 地址绑定的方式，防止 IP 盗用，保证记录数据的真实性、准确性等。

由于网络管理的复杂性，建立一个综合智能化程度高的网络管理系统非常必要，这样不仅可降低尺寸，网络管理员的要求减少系统使用的培训，同时可提高管理的效率。但是，网络管理是一项复杂的工程，真正完全智能化网络管理是自动定位故障并自动处理故障，这是网络管理发展的目标。

11.5　网络故障诊断与排除

现在网络的复杂性日益增大，多种协议的环境正在导致越来越多的问题。对于许多机构来说，互联网络故障排除已经成为一个重要的课题。有理由认为有必要采用系统的方法来解决网络互联过程中出现的问题。

11.5.1　使用系统的故障排除方法

互联网络发生故障所造成的损失可能是灾难性的。修复发生故障的网络或者遭破坏的网络给网络工程师和网络管理员带来了难以想象的压力。在这种情况下，使用特殊的专门技术和所掌握的技巧迅速恢复网络的功能是非常有价值的。

然而，这些专门技术需要深入、详细、广泛地掌握互联网知识。孤立、零散、不系统的故障排除很难使对互联网知识的掌握达到如此的深度和广度。

除非已经知道如何解决问题，否则不系统的故障排除方法只会导致在网络故障现象、互相依赖和偶然性的迷宫中浪费时间。相反，系统的故障排除方法，使你经历掌握详细情况、分析可能原因、针对原因采取行动和观测测试结果的过程，这有助于你详细地了解网络迷宫。故障排除模型的总体思想是系统地将由故障可能的原因所构成的一个大集合缩减成一个小的子集或者直接确定故障起因。然后，你就可以排除故障并恢复网络的功能。问题解决之后，通过记录该事例所形成的系统故障排除方法有助于汲取、保存和交流排除故障过程中所获得的经验。

使用这样的系统故障排除模型提高了机构的专门技术，减少了解决今后类似问题所花

费的时间。提高专门技术和协作的这种转变可以减轻支撑关键的、复杂的互联网过程中的工作压力。

11.5.2 互联网络的复杂性

随着越来越多的先进技术和服务引入到信息处理和通信领域之中，设计、管理和维护互联网络的工作正变得日益复杂。

历史上，网络体系结构是以主机为中心的。基于大型主机的体系结构随着客户机/服务器范例的出现演变成为分布式处理系统。新的应用，如视频、音频和多媒体，正越来越普及，而且由于客户机和服务器中处理器运算速度的提高，这些应用是可行的。其结果造成用户桌面系统需要高速的连接，如专用的 10 Mb/s 以太网、100 Mb/s 以太网、1000 Mb/s 光纤分布式数据接口或更高。为了适应增大的网络负荷的传输，通信公司正在实现诸如 ISDN、帧中继和 ATM 的业务。

多种多样的专有协议加大了互联网络的复杂性。国际标准化组织开放系统互联参考模型的目标是在不同销售商的系统之间提供兼容性和互操作性。在理论上提供共同的体系结构并消除互通的障碍。虽然许多厂家根据七层 OSI 模型制定其协议的结构，但是所有厂家的产品进行无缝隙衔接还很不现实。

由于上述因素，当今的互联网络是复杂的。互联网络已成为协议、技术、介质和拓扑的混合体。复杂性的增加造成不同的连接行问题和性能问题有可能出现。不同的问题需要系统的故障排除模型。

11.5.3 故障排除模型

现代网络的复杂性和对至关重要的无故障运行时间的需求增加了解决连通性和性能问题的压力。处理网络互联问题的最好办法是开发一个标准的故障排除方法学。图 11-18 提出的故障排除模型是这种方法学的一个范例。故障排除时有序的思路有助于解决所遇到的任何问题。随着用户所在的机构支撑其互联网络，该模型也有助于用户和所在机构全面提高专门技术。

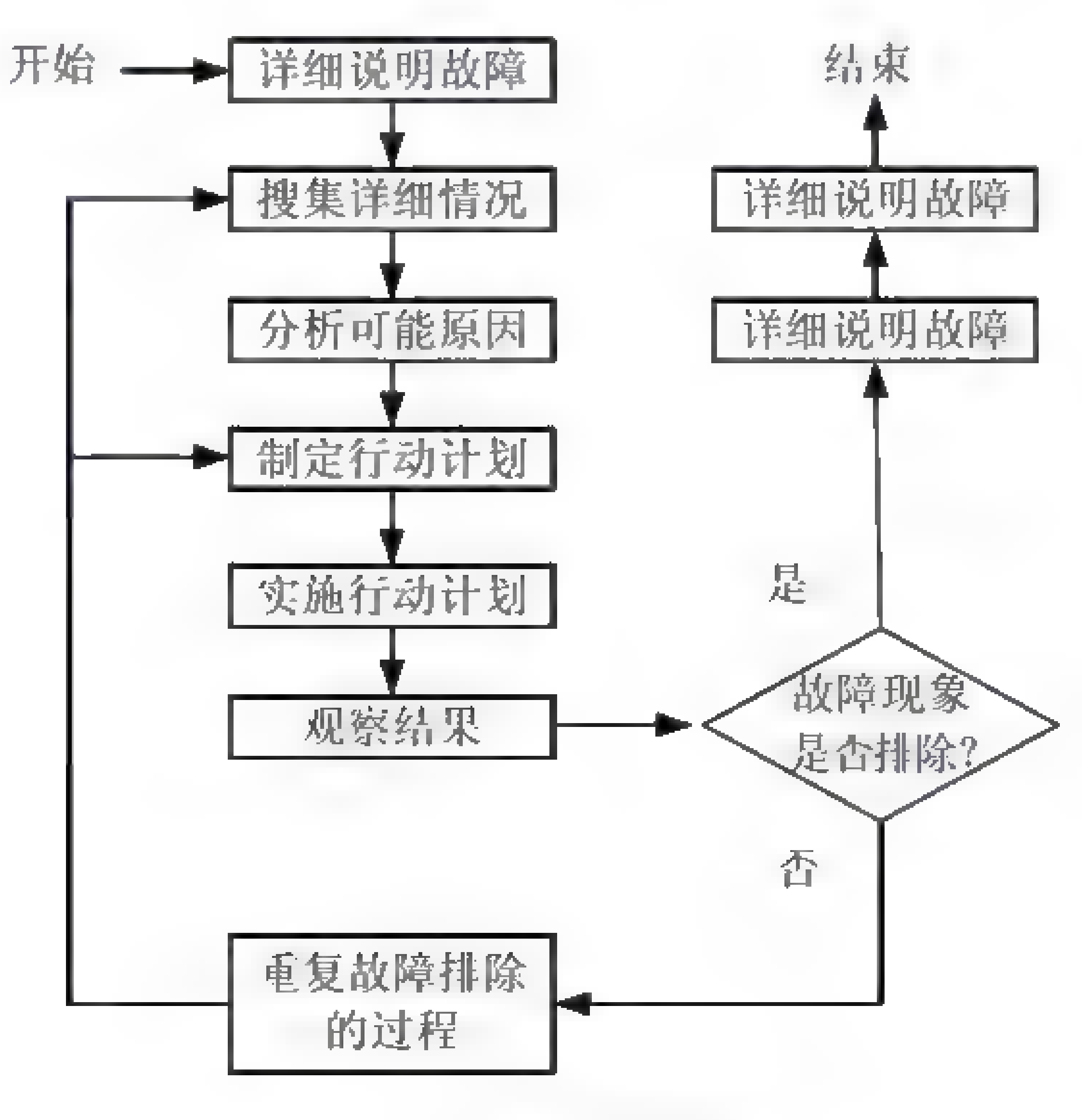


图 11-18 故障排除模型

图 11-18 列出了一系列步骤。这些步骤可以分为以下几个故障排除阶段。

① 确保具有明确的、充分的问题描述。

② 全面搜集相关情况并分析可能的原因。

③ 针对可能性最大的原因制定和实施一个操作计划，然后观察其结果。

④ 如果故障现象没有排除，尝试另一项操作计划。

⑤ 如果故障现象消除了，记录并整理排除故障的方法。

> **注意：** 这个故障排除模型是你能够采用的许多同类模型中的一种。如果用户已经在使用另外一种模型，则应该继续使用它。如果用户过去的经历中没有系统地处理过问题或没有考虑过使用故障排除模型，用户应该采纳如本章所描述的一种方案。

11.5.4　故障排除步骤

我们通过一个示例来学习故障排除的各个步骤。

【例 11-2】　网络故障情况如图 11-19 所示，该网络使用 TCP/IP 协议簇，而且发生了一个故障。故障现象是主机 1 和主机 2 的用户得不到主机 A 或主机 B 的任何响应。如何排除这种故障？

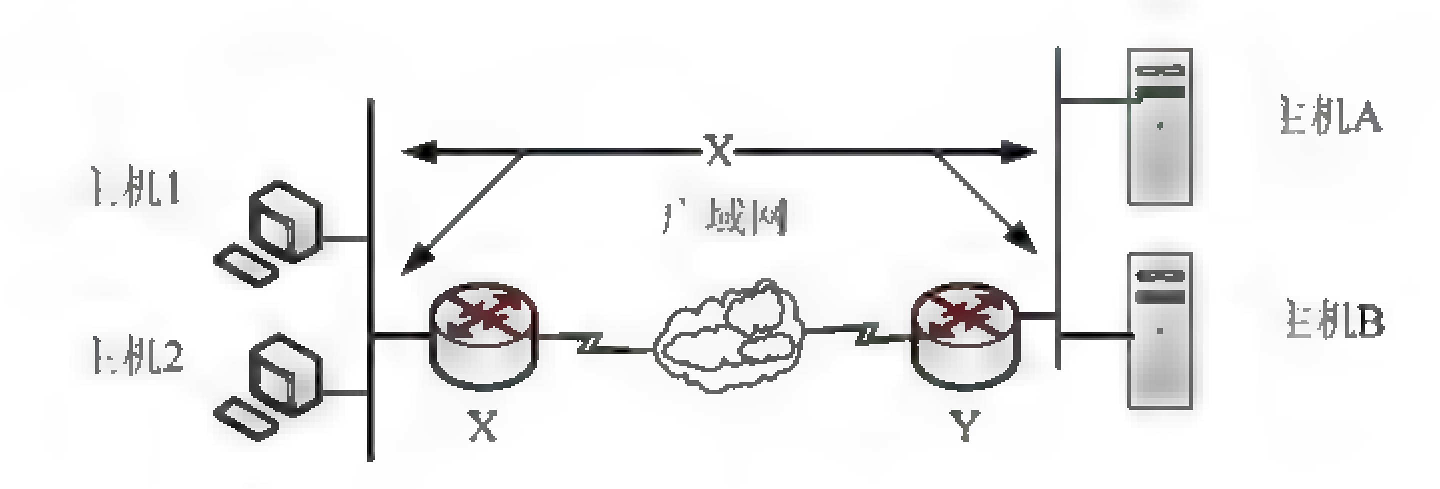


图 11-19　网络故障排除实例

（1）详细说明故障

分析互联网络故障时，按照一组故障现象及相关原因详细说明故障，以便对故障作清晰的描述。参照为网络制定的基准指标进行故障描述。做这项工作首先要观察总体的故障现象，然后确定可能有哪几类原因会导致这些故障现象。

下面是主机 1 和主机 2 通信故障可能的原因。

① 主机 1 和主机 2 安装的网卡有故障。

② 主机 1 和主机 2 需要缺省网卡，但是没有做配置。

③ 主机 1 和主机 2 或路由器 X 中存在错误配置的子网掩码。

④ 网络 R 连接了故障的设备，它在以太网电缆上导致了太多的冲突。

⑤ 路由器 X 或路由器 Y 访问控制表配置不正确，导致来自受影响主机的数据流被阻塞。

⑥ 广域网连接发生故障。

⑦ 路由器没有配置有效的协议映射声明。

⑧ 主机 A 和主机 B 没有做识别主机 1 和主机 2 的配置。

也许还有其他可能的原因，但是首先应该注意那些被认为是造成故障现象的主要原因。

系统的故障排除方法由一系列步骤组成。这些步骤中的第一组步骤是一定要清晰、充

分地说明故障，然后全面搜集相关的详细情况。在最终用户报告的情况是重要的；但是，全面详细的故障描述可能具有更广泛的基础。如果可能，根据关于自己的互联网络的知识继续进行下去，并尽力自己了解故障。进行故障描述必须参照为网络制定的各项基准指标。应当知道当网络按照预期的状况运行时，网络指示器的显示。还必须知道自上一次表现出基准性能以来，网络有哪些方面发生了改变。

（2）搜集详细情况

故障排除的第二步骤是搜集有助于查找故障原因的详细情况。向受到影响的用户、网络管理员、经理和网络所涉及的其他关键人员提出问题。尽量确定是否有人知道做出改动的地方。完整地记录获得的全部信息。

分析故障时，假定搜集到了下列情况。

① 主机 3 和主机 4 能够与主机 A 和主机 B 通信。

② 主机 1 和主机 2 能够与主机 3 和主机 4 通信。

③ 主机 1 能够与主机 2 通信。

④ 为了识别与主机 1 和主机 2 通信，主机 A 和主机 B 进行了正确的配置。

（3）分析可能性

利用用户搜集的数据和所掌握知识及关于自己的互联网络环境中其他设备的知识，可以确定一个范围，这有助于查找故障的原因。通过划定范围，用户只需注意与某一故障或故障情况相关的那一部分产品、介质和主机。

根据故障示例中所搜集的情况能够排除几种可能的原因。

① 主机 1 和主机 2 安装的网卡有故障。可以不考虑这个可能的原因，因为主机 1 和主机 2 可以通信。

② 主机 1 和主机 2 需要缺省网关，但是没有做配置。可以不考虑这个问题的原因，因为主机 1 和主机 2 能够与主机 3 和主机 4 通信。

③ 主机 1 和主机 2 或路由器 X 中存在错误配置的子网掩码。可以不考虑这个可能的原因，因为主机 1 和主机 2 能与主机 3 和主机 4 通信。

④ 网络 R 连接了有故障的设备，它在以太网电缆上导致了太多的冲突。可以不考虑这个可能的原因，因为主机 1 和主机 2 能够与主机 3 和主机 4 通信。而且，主机 1 和主机 2 可以通信。

⑤ 路由器 X 和路由器 Y 访问控制表配置不正确，导致来自受影响主机的数据流被阻塞。这仍然是一种可能的原因，可以根据所搜集这个原因。

⑥ 广域网连接发生故障。可以不考虑这个问题的原因，因为主机 3 和主机 4 能够与主机 A 和主机 B 通信。

⑦ 路由器没有配置有效的协议映射声明。可以不考虑这个可能的原因，因为主机 3 和主机 4 能够与主机 A 和主机 B 通信。

⑧ 主机 A 和主机 B 没有做识别主机 1 和主机 2 的配置。可以不考虑这个可能的原因，因为为了识别与主机 1 和主机 2 通信，主机 A 和主机 B 进行了正确的配置。搜集情况时我们已经检查了这项内容。

故障的范围被缩小为：路由器 X 或路由器 Y 中配置的访问控制表可能阻塞了到达/来自主机 1 和主机 2 的数据流。

（4）制定操作计划

根据对故障示例的分析，已经确定最有可能的原因是某个路由器中访问控制表配置不正确，从而阻塞了到达/来自主机 1 和主机 2 的数据流。

针对这种原因的操作计划是检查每台路由器当前的配置，判断所出现的访问控制表是否正确。

分析了配置之后，试着修复配置错误的访问控制表或者暂时禁用访问控制表。

> 注意：切记禁用访问控制表会停止访问控制表提供的安全功能。

（5）实施操作计划

具体和明确地制定和实施操作计划是非常重要的。操作计划必须确定执行的一组步骤，而且每个步骤必须认真更改各个变量。制定还原的计划以使网络能够回到先前已知的状态，这一点很重要。

（6）观察操作计划的结果

对结果做出分析之后，必须判断问题是否已得到解决。如果解决了问题，那么这一步就是故障排除模型中不断重复过程的退出点。如果问题未得到解决，则必须利用这些结果更好地调整计划，直到获得了适当的解决办法。

对于上述故障示例，对一个变量进行操作，即重新配置了访问控制表或暂时禁用了它，并观察操作结果。现在主机 1 和主机 2 能够访问主机 A 和主机 B 么？如果能，则问题得到了解决，诊断过程到此结束。然而，如果主机 1 和主机 2 仍不能访问主机 A 和主机 B，那么必须进行下一步骤。

（7）重复故障排除的过程

为了达到模型中问题/解决办法重复过程的退出点，必须努力不断缩小可能原因的范围，直到只有一个原因为止。

所以，缩小了可能原因的清单之后（由于实施前面的操作计划并观察结果），以基于最新（缩小了或扩大了）可能原因清单的新操作计划为七点，重复这个故障排除的过程。重复这一过程直到找到了解决办法。问题的解决可能需要修改主机配置、路由器或介质。

> 注意：取消所做的任何无效的“修复”是非常重要的。一次只修改一个变量。而且，如果在网络中一次做太多的修改，将会导致网络性能和策略的降低。这就是制定还原计划以取消修改并将网络恢复到先前状态的重要原因。

故障排除过程必须反复进行直到问题得到解决。系统地排除每一种可能的原因，直到分离并确定故障的原因，此时就可以修复故障。

（8）排除故障

如果找到了故障的真正起因，就可以完成故障的排除并作文字记录。然而，当用户尽力排除网络故障时，如果针对自己的网络环境分析了所有的常见原因并采取了所有的一般性措施，那么用户最后寻求的帮助是与自己的路由器技术支持代表联系。应该就故障准备必要的情况报告，这有助于技术支持代表判断故障可能的原因。

本示例的目标之一就是以最少的网络停用时间和外部干预为代价，帮助用户涉及自己的进行数据搜集、故障排除和故障预防的步骤。即使本模型中不断重复的故障排除过程看上去很费时间，但是随着你的故障排除技术的成熟，这个过程将变得自然而然，而且没有

必要一步一步地严格遵照流程图进行。

一旦故障现象不再出现，则故障可能已经排除。无论何时都需要对所做的工作进行文字记录，包括以下内容。

① 记录采取了哪些步骤（例如，你是否请其他人参与，如本机构中的其他工程师或管理员，或者 Cisco 技术支持中心）。

② 如果有迹象表明必须取消已采取的行动，则记录还原迹象。

③ 建立历史记录，便于今后参照（例如，帮助自己回忆、帮助其他人了解曾经发生过什么故障）。这项记录为今后解决类似问题提供了便利。

11.5.5 故障排除

在进行故障排除、查明故障原因并恢复网络正常运行的过程中，用户运用了所掌握的关于自己网络的专门技术。为了有效地进行故障排除，必须充分了解自己的网络，而且能够迅速、有效地与网络管理所涉及的关键人员以及受故障影响的人员进行沟通。

① 你持有自己互联网络精确的物理连接图和逻辑连接图吗？你所在机构或部门是否持有最新的简述网络中所有设备物理位置和连接关系的互联网络连接图以及描述网络地址、网络号和子网等数据逻辑连接图？

② 你持有自己网络中所运行的全部网络协议的清单吗？对于每一种运行的协议，你是否持有网络号、子网、域、区及上述数据相关内容的清单？

③ 你知道对哪些协议进行路由吗？对于每一种作路由的协议，你是否掌握了正确的、最新的路由器配置？

④ 你知道对哪些协议进行桥接吗？在这些网桥中是否配置了过滤器，你了解这些配置情况吗？

⑤ 包括全因特网的全部连接在内，你知道与外部网络的所有连接点吗？对于每一条外部网络连接，你知道采用了哪一种路由协议吗？

⑥ 你知道自己网络既定的基准性能指标吗？你所在的机构是否记录了网络正常的状态和性能以便能将当前的故障与基准性能进行比较？网络正常运行时你所预期的正常基准活动有哪些？自从上一次网络达到基准指标以后，对网络做了哪些事情、增加了哪些新设备和软件、重新做了哪些配置？

⑦ 故障涉及了哪些特殊的应用特性和数据流传需求？哪些过去的故障排除事例适用于当前的情况或者有所帮助？

系统的故障排除方法能够帮助节省在复杂的、相互联系的网络细节迷宫中浪费的时间。由于网络是机构中的战略性工具，寻找捷径是很实际的情况。这些捷径往往出自以前的专门技术，而这些专门技术则可能从系统的故障排除工作获得。

如果你已经掌握了一种得心应手的系统的故障排除方法，请继续使用它对网络作故障排除。然而，如果你未采取系统的故障排除方法，可以考虑使用本章提出的那些方法。

> **提示：** 为了增进和交流在网络故障排除过程中学到的知识，可采用对故障排除的详细过程作记录的方法。

习题

1. 简单介绍网络管理的功能。
2. 简单网络管理协议 SNMP 的作用是什么？
3. 简单描述 HP OpenView 的管理框架。
4. 列举 5 个常见的网络管理系统。
5. 分析本章介绍的网络管理系统的特点以及优劣性。
6. 简单描述网络故障诊断流程。
7. 简单描述网络故障排除过程。

第 12 章　计算机网络安全

教学提示

计算机网络是信息社会的基础，已经进入社会的各个角落。然而网络本身的开放性、跨国界等特性，在给人们带来便利的同时，也带来了不容忽视的安全问题。网络的安全问题正面临着日益严峻的威胁。

本章主要介绍网络安全的基本概念，分析了 Internet 中存在的主要安全隐患及常见的威胁与攻击。从技术角度较深入探讨了计算机网络的安全防范措施。并根据网络安全的特点讲述了防火墙技术、入侵检测技术等内容。

教学重点

网络安全是一个综合学科领域，涉及数学、电子、通信和计算机等诸多学科知识。网络安全研究的内容很多，涉及安全体系结构、安全协议、密码理论、安全监控和应急措施等，其中密码技术是网络安全的关键技术，防火墙技术是保护计算机网络安全的最成熟、最早产品化的技术措施，入侵检测是对防火墙及其有益的补充，能够帮助网络系统快速发现网络攻击，扩展了系统管理员的安全管理能力。

12.1　网络安全基础

网络安全泛指网络系统的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改和泄漏。系统连续可靠正常地运行，网络服务不被中断。

网络安全的内容包括了系统安全和信息安全两个部分。系统安全主要指网络设备的硬件、操作系统和应用软件的安全；信息安全主要指各种信息的存储、传输的安全，具体体现在保密性、完整性及不可抵赖性上。

12.1.1　网络安全的组成

从内容上讲，网络安全大致包括 4 个方面。

（1）网络实体安全

保证网络系统各种设备的物理安全是整个网络系统安全的前提。网络实体安全是指在物理媒介层次上对存储和传输的信息加以保护，它是保护计算机网络设备、设施免遭地震、水灾和火灾等环境事故以及人为操作错误或各种计算机犯罪行为而导致破坏的过程。

（2）软件安全

保护网络系统不被非法侵入，系统软件与应用软件不被非法复制、篡改和不受病毒的侵害等。

（3）数据安全

保护数据不被非法存取，确保其完整性、一致性、机密性等。

（4）安全管理

运行时突发事件的安全处理等，包括计算机安全技术，建立安全管理制度，开展安全审计，进行风险分析等。

从特征上看，网络安全包括 5 个基本要素如下。

- 机密性：确保内容不暴露给未授权的实体。
- 完整性：只有得到允许的人才能够修改数据，并能判别数据是否已被篡改。
- 可用性：得到授权的实体在需要时可以访问数据，即攻击者不能占用所有资源阻碍授权者工作。
- 可控性：可以控制授权范围内的信息流向以及行为方式。
- 可审查性：对出现的网络安全问题提供调查的依据和手段。

12.1.2　影响网络安全的因素

1. 网络系统自身的脆弱性

所谓系统的脆弱性是指系统的硬件资源、通信资源、软件及信息资源等，因可预见或不可预见甚至恶意的原因，导致系统受到破坏、泄漏和功能失效，从而使网络处于异常状态，甚至导致崩溃、瘫痪等。计算机网络本身由于系统主体和客体的原因存在不同程度的脆弱性。

（1）硬件系统

网络硬件系统的安全隐患主要来源于设计，主要表现为物理安全方面的问题。各种计算机或者网络外围设备，除了难以抗拒的自然灾害外，温度、湿度、静电和电磁场等都有可能造成信息的泄漏或损坏。

（2）软件系统

软件系统的安全隐患来源于设计和软件工程中的问题。软件设计中的疏忽可能留下安全漏洞，比如前一段的“冲击波”病毒就是针对操作系统的漏洞实施攻击；软件设计不按照信息系统安全等级进行模块化设计，导致软件的安全等级不能达到要求的等级；软件工程实现中造成的软件系统内部逻辑错误等等。软件系统的安全隐患主要表现在操作系统、数据库系统和应用软件上。

（3）网络和通信协议

目前网络中普遍实用的 TCP/IP 协议架构未能全面考虑安全问题，不能提供人们所需要的安全性和保密性。

尽管 TCP/IP 经历了一次又一次的改版、升级，但因协议本身的不足以及在修订中考虑到软件可继承性等原因，仍然未能彻底解决其自身的安全性问题。主要包括如下。

- 缺乏用户身份鉴别机制
- 缺乏路由协议鉴别机制
- 缺乏保密性
- TCP/UDP 的缺陷
- TCP/IP 服务的脆弱性

2. 安全威胁

安全威胁是指某个人、物、事件或概念对某一资源的机密性、完整性、可用性或合法性所造成的危害。安全威胁可分为故意威胁（如黑客渗透）和偶然威胁（如信息被发往错误的地址）两类。故意威胁又可进一步分为被动威胁和主动威胁两类。

（1）基本威胁

网络安全的基本目标是实现信息的机密性、完整性、可用性和合法性。4 个基本的安全威胁直接反映了这 4 个安全目标。一般认为，目前网络存在的威胁主要表现如下。

- 信息泄漏或丢失

这是针对信息机密性的威胁，它指敏感数据在有意或无意中被泄漏出去或丢失，它通常包括：信息在传输中丢失或泄漏（如“黑客”们利用电磁泄漏或搭线窃听等方式可截获机密信息，或通过对信息流向、流量、通信频度和长度等参数的分析，推出有用信息，如用户口令、账号等重要信息）；信息在存储介质中丢失或泄漏；通过建立隐蔽通道等窃取敏感信息等。

- 破坏数据完整性

以非法手段窃得对数据的使用权，删除、修改、插入或重发某些重要信息，以取得有益于攻击者的响应；恶意添加、修改数据，以干扰用户的正常使用。

- 拒绝服务

它不断对网络服务系统进行干扰，改变其正常的作业流程，执行无关程序使系统响应减慢甚至瘫痪，影响正常用户的使用，甚至使合法用户被排斥而不能进入计算机网络系统或不能得到相应的服务。

- 非授权访问

没有预先经过同意就使用网络或计算机资源被看作非授权访问，如有意避开系统访问控制机制，对网络设备及资源进行非正常使用，或擅自扩大权限，越权访问信息。它主要有以下几种形式：假冒、身份攻击、非法用户进入网络系统进行违法操作、合法用户以未授权方式进行操作等。

（2）渗入威胁和植入威胁

在基本威胁中，目前常见的可以实现的威胁主要包括两类：渗入威胁和植入威胁。渗入威胁主要有：假冒、旁路控制和授权侵犯。植入威胁主要有：特洛伊木马、陷门。

- 渗入威胁

假冒：这是大多数黑客采用的攻击方法。某个未授权实体使守卫者相信它是一个合法的实体，从而攫取该合法用户的特权。

旁路控制：攻击者通过各种手段发现本应保密却又暴露出来的一些系统“特征”。利用这些“特征”，攻击者绕过防线守卫者渗入系统内部。

授权侵犯：也称为“内部威胁”，授权用户将其权限用于其他未授权的目的。

- 植入威胁

特洛伊木马：攻击者在正常的软件中隐藏一段用于其他目的的程序，这段隐藏的程序段常常以安全攻击作为其最终目标。例如，一个外表上具有合法目的的软件应用程序，如文本编辑器，它还具有一个暗藏的目的，就是将用户的文件复制到另一个秘密文件中，这种应用程序称为特洛伊木马，此后，植入特洛伊木马的那个人就可以阅读该用户的文件了。

陷门：陷门是在某个系统或某个文件中设置的“机关”，使得在提供特定的输入数据时，允许违反安全策略。例如，一个登录处理子系统允许处理一个特定的用户识别码，以绕过通常的口令检查。

（3）潜在威胁

对各种类型的安全威胁进行分析，可以发现某些特定的潜在威胁，而任意一种潜在威胁都可能导致发生一些更基本的威胁。例如，如果考虑信息泄露这种基本威胁，我们有可能找出以下几种潜在威胁：窃听、通信量分析、人员疏忽和媒体清理。图 12-1 给出了一些典型的威胁以及它们之间的相互关系。

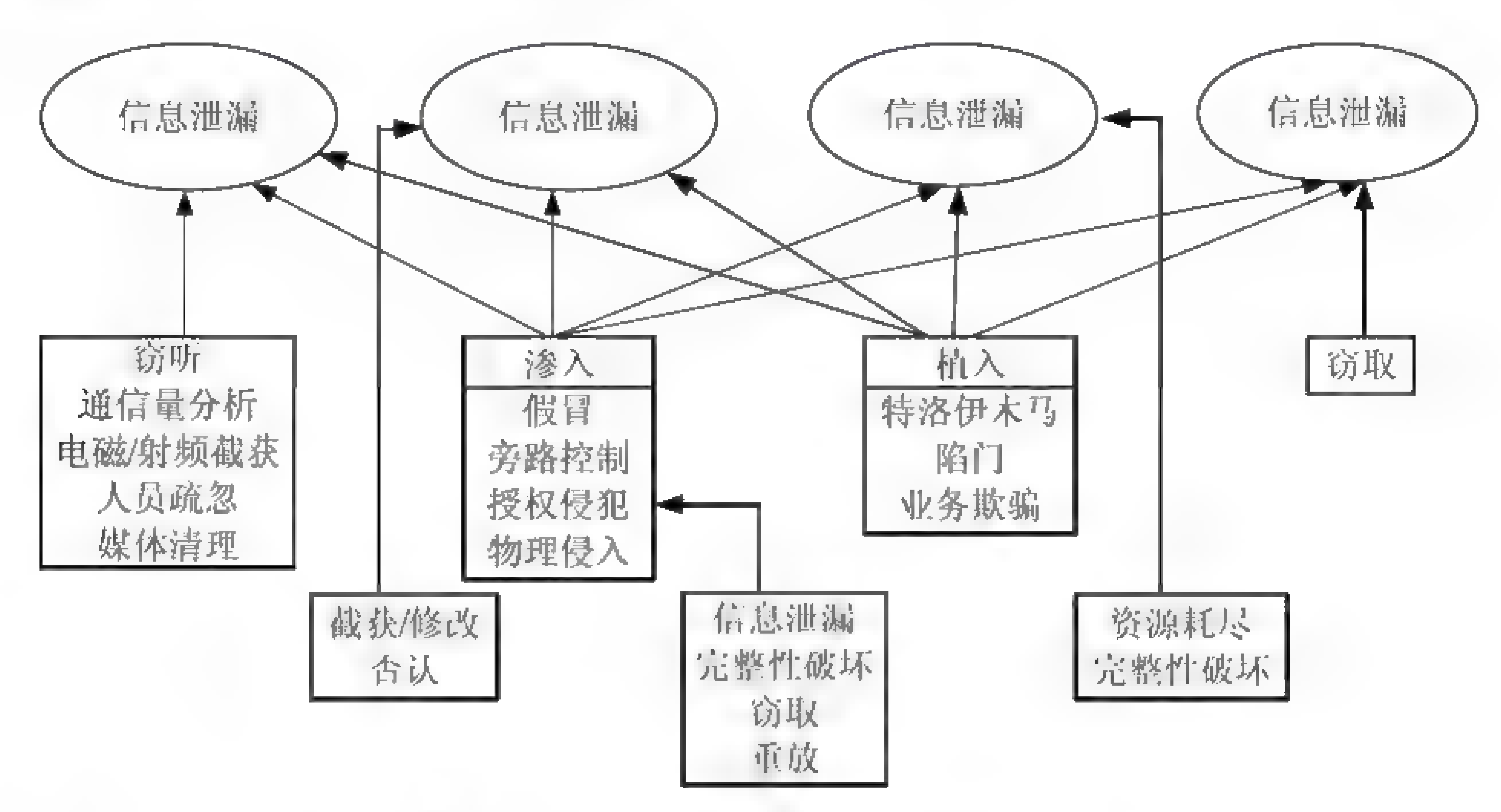


图 12-1　典型的潜在威胁及其相关关系

12.1.3　网络安全服务

1. 保密性

保密性是指网络信息不会泄漏给未授权的用户、实体或过程，即相关信息只被授权用户使用。根据发布消息的内容不同，可以使用几个不同的保护级别。最广泛的保密服务是保护两个用户之间在一段时间内传送的所有数据。例如，如果在两个系统之间建立虚电路，这种广泛的保护可以防止任何用户在虚电路上传送的数据被泄漏。这种保留服务更严密的形式包括对一条消息或消息中特定的域的保护。

保密性的另一方面是保护通信流，以防止被分析。这就要求攻击者看不到通信设备上通信流的来源和目的地、频率、长度或其他特性。

数据保密性服务实现的主要手段包括以下几方面。

（1）物理保密

利用各种物理方法，如限制、隔离、掩蔽和控制等措施，保护信息不被泄漏。

（2）防窃听

使对手侦听不到有用的信息。

（3）防辐射

防止有用的信息以及各种途径辐射出去。

（4）信息加密

在密钥的控制下，用加密算法对信息进行加密处理。即使对手得到了加密后的信息，也会因为没有密钥而无法读懂有效信息。

2. 身份验证

身份验证（也称身份鉴别）服务的目的在于保证消息的可靠性。在只有一条消息的情况下，验证服务的功能就是要保证信息接收方接收的信息确实是从它声明的来源发出的。在进行交互的过程中，如果终端连接到主机上，需要涉及两个方面。首先，在连接的初始化阶段，此服务应保证两个实体的可靠性（每个实体都是所声明的实体）；其次，此服务还应保证第三方不能靠伪装成两个合法实体之一来干扰连接，执行未授权的传送或接收。

实现身份认证的主要方法包括口令、数字证书和基于生物特征（比如指纹、声音和虹膜等）的认证等。

3. 完整性

完整性是网络信息未经授权不能进行改变的特性，即网络信息在存储或传输过程中保持不被偶然或故意地添加、删除、修改、伪造、乱序和重放等操作破坏和丢失的特征。完整性是一种面向信息的安全性，它要求保持信息的原样，即信息的正确性生成，正确存储和正确传输。

完整性与保密性不同，保密性要求信息不被泄漏给未授权的人，而完整性则要求信息不受到各种原因的破坏。影响网络信息完整性的主要因素是设备故障、误码（传输、处理或存储过程中产生的误码，定时的稳定度或精度降低造成的误码，各种干扰源造成的误码）、人为攻击和计算机病毒等。

保障网络信息完整性的主要方法有如下几种。

- 良好的协议：通过各种安全协议可以有效地检测出被复制的信息，被删除的字段，失效的字段和被修改的字段。
- 密码校验和：它是抗篡改和防止传输失败的重要手段。
- 数字签名：保障信息的真实性，保证信息的不可抵赖性。
- 公证：请求网络管理或中介机构证明信息的真实性。

4. 不可抵赖性

不可抵赖性是指防止发送方或接收方否认消息的发送或接收。当消息发出时，接收方可以证实消息确实是从声明的发送方发出。与此类似，当接收到消息时，发送方也能证实消息确实由声明的接收方接受了。

实现不可抵赖性的主要手段有数字签名等方法。

5. 访问控制

在网络安全环境中，访问控制能够限制和控制通过通信链路对主机系统和应用的访问。为了达到这种控制，每个想获得访问的实体都必须经过鉴别或身份验证，这样才能根据个体来制定访问权利。

访问控制主要有 3 种类型：自主访问控制、强制访问控制和基于角色的访问控制。

6. 可用性

一般地，可用性是指当用户需要使用网络时，网络能够及时地提供服务。

可用性是网络信息可被授权实体访问并按需求使用的特性，即网络信息服务在需要时，允许授权用户或实体使用的特性，或者是网络部分受损或需要降低使用时，仍能为授权用户提供有效服务的特性。可用性是网络信息系统面向用户的安全性能。网络信息系统最基本的功能是向用户提供服务。而用户的需求是随机的、多方面的，有时还有时间要求。可

用性一般用系统正常使用时间和整个工作时间之比来度量。

可用性通过以下手段来保证。

- 身份的识别与确认：一般通过用户名和密码进行识别。
- 访问控制：对用户的权限进行控制，只能访问相应权限的资源，防止或限制经隐蔽通道的非法访问。
- 业务流控制：利用均分负荷方法，防止业务流量过度集中而引起网络阻塞，如大型的 ISP（因特网服务提供者）提供的电子邮件服务，一般都有几个邮件服务器进行负载均衡。
- 路由选择控制：选择那些稳定可靠的子网、中继线或链路等。
- 审计跟踪：把网络信息系统发生的所有安全事件情况存储在安全审计跟踪之内，以便能够根据日志分析原因，分清责任，并且及时采取相应的措施。

12.1.4　安全评估准则

一个安全产品的购买者怎样才能知道产品的设计是否足够安全和适当呢？为了帮助计算机用户区分和解决计算机网络安全问题，不同的组织各自制定了一套安全评估准则。一些重要的安全评估准则如下。

- 美国国防部和国家标准技术研究所的可信计算机系统评估准则（TCSEC）
- 欧洲共同体的信息技术安全评测准则（ITSEC）
- 国际标准 ISO/IEC 15408（CC）
- 美国信息技术安全联邦准则（FC）

12.2　加密与认证技术

计算机技术和微电子技术的发展为密码学理论的研究和实现提供了强有力的手段和工具。密码学已渗透到雷达、导航、遥控、通信、电子邮政、计算机、金融系统、各种管理信息系统甚至家庭等各部门和领域，也不仅仅是单纯为了“保密”，还有认证、数字签名等新功能。

数据加密是计算机网络安全很重要的一个部分。由于因特网本身的不安全性，我们不仅对口令进行加密，有时也对在网上传输的文件进行加密。为了保证电子邮件的安全，人们采用了数字签名这样的加密技术，并提供基于加密的身份认证技术。数据加密也使电子商务成为可能。

12.2.1　密码算法与密码体制

密码学是保密学的一部分。保密学是研究密码系统或通信安全的科学，它包含两个分支：密码学和密码分析学。密码学是对信息进行编码实现隐蔽信息的一门学问。密码分析学是研究分析破译密码的学问。两者相互独立，而又相互促进，正如病毒与反病毒技术一样。

采用密码技术可以隐藏和保护需要保密的消息，使未授权者不能提取信息。需要隐藏的消息称为明文。明文被变换成另一种隐蔽形式就称为密文。这种变换称为加密。加密的

逆过程，即从密文恢复出明文的过程称为解密。对明文进行加密时采用的一组规则称为加密算法。对密文解密时采用的一组规则称为解密算法。加密算法和解密算法通常都是在一组密钥控制下进行的，密钥决定了从明文到密文的映射，加密算法所使用的密钥称为加密密钥，解密算法所使用的密钥称为解密密钥。

密码体制通常从以下 3 个独立的方面进行分类。

- 按明文到密文的转换操作可分为置换密码和易位密码。
- 按明文的处理方法可分为分组密码和序列密码。
- 按密钥的使用个数可分为对称密码体制和非对称密码体制。

12.2.2 对称加密算法

1. 对称加密算法概述

如果发送方使用的加密密钥和接收方使用的解密密钥相同，或者从其中一个密钥易于得出另一个密钥，这样的系统就叫做对称的、单密钥或常规密码系统。

对称加密使用单个密钥对数据进行加密或解密，其特点是计算量小、加密效率高。但是此类算法在分布式系统上使用较为困难，主要是密钥管理困难，从而使用成本较高、安全性能也不易保证。这类算法的代表是在计算机网络系统中广泛使用的 DES 算法。

2. 对称加密算法基本原理

图 12-2 是对称密码系统模型，其显示了对称密码系统的加密、解密过程。最初的可理解的消息 M 称为明文，发送者将明文转换为人们不能直接理解的无规则和无意义的密文 C。加密器利用密钥 K 作用于明文，产生密文 C。密钥 K 独立于明文，对于相同的明文，不同的密钥产生的密文。可将这个过程表示如下。

$$C = E_K(M)$$

产生密文之后，该密文就能够用于传输。在接收方，使用解密器和相同的密钥 K，密文 C 能被恢复为最初的明文。这个过程可表示如下。

$$M = D_K(C)$$

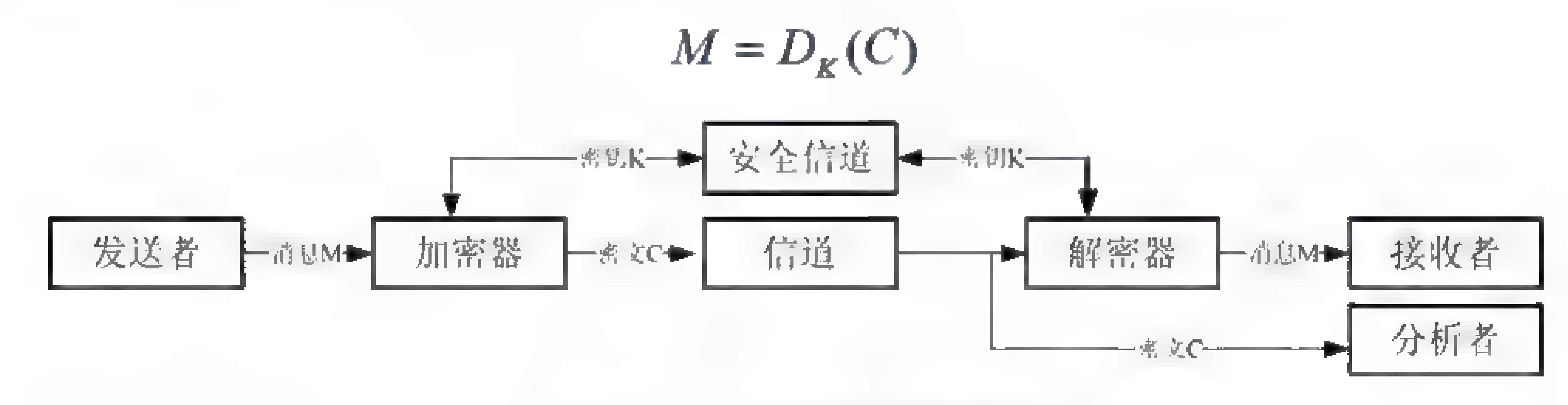


图 12-2 对称密码系统模型

对于分析者来说，可以得到加密、解密算法和从不安全信道上得到密文 C，而不能得到的是通过安全信道传输的密钥 K。这样，对称密码必须满足如下要求。

- 算法要足够强大。
- 不依赖于算法的保密，而依赖于密钥。这就是著名的 Kerckhoff 原则。
- 密钥空间要足够大，且加密和解密算法适用于密钥空间所有的元素。

这也是非对称密码技术必须满足的条件。除此之外，在实际运用中，发送方和接收方必须保证用安全的方法获得密钥的副本。

3. 常用的对称加密算法

目前经常使用的一些对称加密算法有数据加密标准（DES）、TDEA、RC5 和国际数据加密算法（DEA）等。

（1）DES

DES 是美国国家标准和技术局（NIST）在 1977 年采用的数据加密标准，文献号为 FIPS PUB 46。算法本身称为 DEA（数据加密算法）。DES 是最常用的对称加密算法，几乎是事实上的国际标准。DES 的密钥长度为 56 位，分组长度为 64 位。DES 曾被人利用网络计算采用穷举攻击的方法破解过，目前也已经设计出采用穷举攻击在 4 小时内破解 DES 的机器。DES 本身虽已不再安全，但其改进算法的安全性还是相当强的。

（2）TDEA

TDEA（三重 DEA，或称 3DES）最初是由 Tuchman 提出的，在 1985 年的 ANSI 标准 X9.17 中第一次为金融应用进行了标准化。1999 年，TDEA 合并到数据加密标准中，文献号为 FIPS PUB 46-3。TDEA 使用 3 个密钥，并执行 3 次 DES 算法。TDEA 的密钥长度是 168 比特，这就克服了 DES 不能抵制穷举攻击的弱点。TDEA 的缺点是软件实现相对缓慢。

（3）RC5

RC5 是由 Ron Rivest（公钥算法 RSA 的创始人之一）在 1994 年开发出来的。其前身 RC4 的源代码在 1994 年 9 月被人匿名张贴到因特网上，泄露了 RCA 的算法。RC5 是在 RFC 2040 中定义的，RSA 数据安全公司的很多产品都已经使用了 RC5。RC5 的分组长度和密钥长度都是可变的，可以在速度和安全性之间进行折中。

（4）IDEA

IDEA 是在 1991 年由瑞士联邦技术协会的 Xuejia Lai 和 James Massey 开发的。IDEA 以 64 位的明文块进行分组，密钥长度为 128 位，主要采用异或、模加和模乘 3 种运算，容易用软件和硬件实现。IDEA 算法被认为是当今已公开的最好最安全的对称分组密码算法。

12.2.3　公钥加密算法

1. 公钥加密算法概述

如果发送方使用的加密密钥和接收方使用的解密密钥不相同，从其中一个密钥难以推出另一个密钥，这样的系统就叫做非对称的、双密钥或公钥密码系统。

非对称型加密算法的特点是有两个密钥（即公用密钥和私有密钥），只有二者搭配使用才能完成加密解密的全过程。由于非对称算法拥有两个密钥，它特别适用于分布式系统中的数据加密，在因特网中得到广泛应用。其中公用密钥在网上公布，供发送方对数据加密时使用。而用于解密的相应私有密钥则由数据的接受方妥善保管。非对称加密的另一用法是“数字签名”，用于防止通信一方的抵赖行为。在网络系统中得到应用的非对称加密算法有 RSA 算法和美国国家技术标准研究所提出的数字签名算法 DSA。非对称加密在分布式系统中应用时需注意的问题是如何管理和确认公用密钥的合法性。

2. 公钥加密算法基本原理

公开密钥密码系统的理论基础是数论。在公开密钥算法中，加密/解密是整个算法方案的核心。Diffie 和 Hellman 设想出了这个系统，但是却没有表明这种算法的存在性，他们给出了一个公开密钥密码系统必须满足的条件如下。

通信双方 A 和 B 容易产生出一对密钥（公钥 KU，私钥 KR）。

在知道公钥KU和待加密报文M的情况下，对于发送方A，很容易通过计算产生对应的密文如下。

$$C = E_{KU}(M)$$

接收方B使用私有密钥容易通过计算解密所得的密文，以便恢复原来的报文。

$$M = D_{KR}(C) = D_{KR}[E_{KR}(M)]$$

除A和B以外的其他人即使知道公钥KU，要确定私钥KR在计算上也是不可行的。除A和B以外的其他人即使知道公钥KU和密文C，要想恢复原来的明文M在计算上也是不可行的。这些要求最终可以归结到设计一个单向陷门函数（Trapdoor One-way Function）。

单向函数（One-way Function）是满足下列条件的函数：它将一个定义域映射到值域，使得每个函数值有一个唯一的原像，函数值计算很容易，而逆计算是不可行的。

在密码学中，"容易"是指一个问题可以在多项式函数时间内解决，这个多项式函数是输入长度的函数。不可行是指将一个问题的工作量作为一个函数的输入，函数值的增长速度超过多项式时间。

单向陷门函数，即除非知道某种附加的信息，否则这样的函数在一个方面上容易计算，而在另外的方向上的计算是不可行的。有了附加的信息，函数的逆就可以在多项式时间内计算出来，即有如下式子。

$Y = f_k(X)$　　容易，知道了 k 和 X

$X = f^{-1}{}_k(Y)$　　容易，知道了 k 和 Y

$X = f^{-1}{}_k(Y)$　　不可行，如果知道 Y 而不知道 k

3. 常用公钥加密算法

公钥密码体制的设计比对称密码体制的设计具有更大的挑战性。因为公钥算法是公开的，这为攻击者提供了一定的信息。目前公钥体制的安全基础主要是数学中的难解问题。最流行的有两大类，一类基于大整数因子分解问题，如RSA体制；另一类基于离散对数问题，如Elgamal体制、椭圆曲线密码体制等。

大多数公钥密码体制都会涉及高次幂运算，不仅加密速度慢，而且会占用大量的存储空间。目前许多商业产品采用的公钥算法还有Diffie-Hellman密钥交换、数字签名标准DSS等。

（1）RSA

RSA公钥体制是1978年由Rivest，Shamir和Adleman三个人提出的一个公开密钥密码体制，RSA就是以其发明者的首字母命名的。RSA体制被认为是迄今为止理论上最为成熟完善的一种公钥密码体制。该体制的构造基于Euler定理，它利用了如下的基本事实。寻找大素数是相对容易的，而分解两个大素数的积在计算上是不可行的。

RSA算法的安全性建立在难以对大数提取因子的基础上。所有已知的证据都表明，大数的因子分解是一个极其困难的问题。

与对称密码体制如 DES 相比，RSA 的缺点是加密、解密的速度太慢。因此，RSA 体制很少用于数据加密，而多用在数字签名、密钥管理和认证等方面。

（2）Elgamal 公钥体制

1985 年，El Gamal 构造了一种基于离散对数的公钥密码体制，这就是 Elgamal 公钥体制。Elgamal 公钥体制的密文不仅依赖于待加密的明文，而且依赖于用户选择的随机参数，即使加密相同的明文，得到的密文也是不同的。由于这种加密算法的非确定性，又称其为概率加密体制。在确定性加密算法中，如果破译者对某些关键信息感兴趣，则他可事先将这些信息加密后存储起来，一旦以后截获密文，就可以直接在存储的密文中进行查找，从而求得相应的明文。概率加密体制弥补了这种不足，提高了安全性。

与既能作公钥加密又能作数字签名的 RSA 不同，Elgamal 公钥体制是在 1985 年仅为数字签名而构造的签名体制。美国标准技术研究所采用修改后的 Elgamal 签名体制作为数字签名体制标准。破译 Elgamal 签名体制等价于求解离散对数问题。

（3）背包公钥体制

它是 1978 年由 Merkle 和 Hellman 提出的。背包算法的思路是假定某人拥有大量的物品，重量各不相同。此人通过秘密地选择一部分物品并将它们放到背包中来加密消息。背包中的物品总重量是公开的，所有可能的物品也是公开的，但背包中的物品却是保密的。附加一定的限制条件，给出重量，而要列出可能的物品，在计算上是不可实现的。这就是公开密钥算法的基本思想。

12.2.4　数字信封与数字签名技术

1. 数字信封的概念

数字信封是公钥密码体制在实际中的一个应用，是用加密技术来保证只有规定的特定收信人才能阅读通信的内容。

在数字信封中，信息发送方采用对称密钥来加密信息内容，然后将此对称密钥用接收方的公开密钥来加密（这部分称数字信封）之后，将它和加密后的信息一起发送给接收方，接收方先用相应的私有密钥打开数字信封，得到对称密钥，然后使用对称密钥解开加密信息。这种技术的安全性相当高。数字信封主要包括数字信封打包和数字信封拆解，数字信封打包是使用对方的公钥将加密密钥进行加密的过程，只有对方的私钥才能将加密后的数据（通信密钥）还原；数字信封拆解是使用私钥将加密过的数据解密的过程。

数字信封的功能类似于普通信封，普通信封在法律的约束下保证只有收信人才能阅读信的内容；数字信封则采用密码技术保证了只有规定的接收人才能阅读信息的内容。数字信封中采用了对称密码体制和公钥密码体制。信息发送者首先利用随机产生的对称密码加密信息，再利用接收方的公钥加密对称密码，被公钥加密后的对称密码被称之为数字信封。在传递信息时，信息接收方若要解密信息，必须先用自己的私钥解密数字信封，得到对称密码，才能利用对称密码解密所得到的信息。这样就保证了数据传输的真实性和完整性。

2. 数字签名的概念

数字签名，就是通过在数据单元上附加数据，或对数据单元进行秘密变换，从而使接收者可以确认数据来源和完整性。简单说来，数字签名是防止他人对传输的文件进行破坏，以及确定发信人的身份的手段。

目前的数字签名是建立在公共密钥体制基础上，它是公用密钥加密技术的另一类应用。

它的主要方式是报文的发送方从报文文本中生成一个128位的散列值（又称报文摘要，数字指纹）。发送方用自己的私人密钥对这个散列值进行加密来形成发送方的数字签名。然后，这个数字签名将作为报文的附件和报文一起发送给报文的接收方。报文的接收方首先从接收到的原始报文中计算出128位的散列值，接着再用发送方的公用密钥来对报文附加的数字签名进行解密。如果两个散列值相同，那么接收方就能确认该数字签名是发送方的。通过数字签名能够实现对原始报文的鉴别。

采用数字签名，能确认以下两点：第一，信息是由签名者发送的；第二，信息自签发后到收到为止未曾作过任何修改。这样数字签名就可用来防止电子信息因易被修改而有人作伪，或冒用别人名义发送信息。或发出（收到）信件后又加以否认等情况发生。应用广泛的数字签名方法主要有三种，即RSA签名、DSS签名和Hash签名。这三种算法可单独使用，也可综合在一起使用。

3. 数字签名的传输过程

对电子文件进行数字签名并在网上传输，其技术实现过程大致如下：首先要在网上进行身份认证，然后再进行签名，最后是对签名的验证。

（1）认证

PKI提供的服务首先是认证，即身份识别与鉴别，确认实体即为自己所声明的实体。认证的前提是甲乙双方都具有第三方CA所签发的证书，认证分单向认证和双向认证。

单向认证是甲乙双方在网上通信时，甲只需要认证乙的身份即可。这时甲需要获取乙的证书，获取的方式有两种，一种是在通信时乙直接将证书传送给甲，另一种是甲向CA的目录服务器查询索取。甲获得乙的证书后，首先用CA的根证书公钥验证该证书的签名，验证通过说明该证书是第三方CA签发的有效证书。然后检查证书的有效期及检查该证书是否已被作废（LRC检查）而进入黑名单。

双向认证。双向认证是甲乙双方在网上通信时，甲不但要认证乙的身份，乙也要认证甲的身份。其认证过程与单向认证过程相同。

（2）数字签名与验证过程

网上通信的双方，在互相认证身份之后，即可发送签名的数据电文。数字签名的全过程分两大部分，即签名与验证。即发方将原文用哈希算法求得数字摘要，用签名私钥对数字摘要加密得数字签名，发方将原文与数字签名一起发送给接受方；收方验证签名，即用发方公钥解密数字签名，得出数字摘要；收方将原文采用同样哈希算法又得一新的数字摘要，将两个数字摘要进行比较，如果二者匹配，说明经数字签名的电子文件传输成功。

数字签名原理中定义的是对原文做数字摘要和签名并传输原文，在很多场合传输的原文是要求保密的，要求对原文进行加密的数字签名方法如何实现？这里就要涉及“数字信封”的概念。“电子信封”基本原理是将原文用对称密钥加密传输，而将对称密钥用收方公钥加密发送给对方。收方收到电子信封，用自己的私钥解密信封，取出对称密钥解密得原文。其详细过程如下。

① 发方A将原文信息进行哈希运算，得一哈希值即数字摘要MD。

② 发方A用自己的私钥PVA，采用非对称RSA算法，对数字摘要MD进行加密，即得数字签名DS。

③ 发方A用对称算法DES的对称密钥SK对原文信息、数字签名SD及发方A证书

的公钥 PBA 采用对称算法加密，得加密信息 E。

④ 发方用收方 B 的公钥 PBB，采用 RSA 算法对对称密钥 SK 加密，形成数字信封 DE，就好像将对称密钥 SK 装到了一个用收方公钥加密的信封里。

⑤ 发方 A 将加密信息 E 和数字信封 DE 一起发送给收方 B。

⑥ 收方 B 接受到数字信封 DE 后，首先用自己的私钥 PVB 解密数字信封，取出对称密钥 SK。

⑦ 收方 B 用对称密钥 SK 通过 DES 算法解密加密信息 E，还原出原文信息、数字签名 SD 及发方 A 证书的公钥 PBA。

⑧ 收方 B 验证数字签名，先用发方 A 的公钥解密数字签名得数字摘要 MD。

⑨ 收方 B 同时将原文信息用同样的哈希运算，求得一个新的数字摘要 MD′。

⑩ 将两个数字摘要 MD 和 MD′ 进行比较，验证原文是否被修改。如果二者相等，说明数据没有被篡改，是保密传输的，签名是真实的；否则拒绝该签名。

这样就做到了敏感信息在数字签名的传输中不被篡改，未经认证和授权的人，看不见原数据，起到了在数字签名传输中对敏感数据的保密作用。

12.2.5　身份认证技术

网络的安全性常取决于能否正确地验证通信或终端用户的个人身份，如机要部门或地区的进入、自动出纳机提款以及各种计算机资源系统的介入都需要对用户的个人身份进行识别认可。

认证是验证通信用户或终端个人身份最重要的安全服务之一，其他所有安全服务都依赖于认证服务。身份认证是用来获得对谁或对什么事情信任的一种方法。

身份认证大致可分为 3 种：

- 个人知道的某种事物，如口令、账号和个人识别码（PIN）等。
- 个人持证（也称令牌），如图章、标志、钥匙和护照等。
- 个人特征，如指纹、声纹、手形、视网膜、血型、基因、笔迹、习惯性签字等。

12.3　防火墙技术

防火墙就像一个重要单位的门卫一样，要求来访者填上自己的姓名、来访目的、来访事件和拜访何人等。虽令人生厌，但却必不可少。防火墙也一样，它是保证企业内部网络安全的第一道关卡。

为了保障网络安全，防止外部网对内部网的侵犯，常在内部网络与外部公共网络之间设置防火墙。一方面最大限度地让内部用户方便地访问公共网络，另一方面尽可能地防止外部网对内部网的非法入侵。

防火墙总体上分为数据包过滤和应用网关等几大类型。

（1）数据包过滤技术是在网络层对数据包进行选择

通过检查数据流中每个数据包的源地址、目的地址、所用的端口号和协议状态等因素，或者它们的组合来确定是否允许该数据包通过。它通常安装在路由器上。

（2）应用网关是在网络应用层上建立协议过滤和转发功能

它针对特定的网络应用服务协议使用指定的数据过滤逻辑，并在过滤的同时，对数据包进行必要的分析、登记和统计，形成报告。实际中的应用网关通常安装在专用工作站系统上。

12.3.1 防火墙的基本概念

防火墙一般设置在可信任的企业内部网和不可信任的公共网之间，它可以设定哪些内部服务可以被外界访问，外界的哪些人可以访问内部的哪些服务，以及哪些外部服务可以被内部人员访问。所有来往公共网络的信息都必须经过防火墙的检查。防火墙必须只允许授权的数据通过，并且本身能够免于渗透。

1. 防火墙的定义

防火墙是指为了增强机构内部网络的安全性而设置在不同网络或网络安全域之间的一系列部件的组合。它可通过监测、限制、更改跨越防火墙的数据流，尽可能地对外部屏蔽网络内部的信息、结构和运行状况，以此来实现网络的安全保护。

在逻辑上，防火墙是一个分离器，一个限制器，也是一个分析器，本质上是一个独立的进程或一组紧密结合的进程，通过监控内部网和公共网络之间的任何活动，确保一个单位的内部网与因特网之间所有的通信均符合该单位的安全策略。

防火墙的设计目标如下。

- 进出内部网的通信量必须通过防火墙。
- 只有那些在内部网安全策略中定义为合法的通信量才能够进出防火墙。
- 防火墙自身应该能够防止渗透。

2. 防火墙的优点

防火墙不仅仅是路由器、堡垒主机或任何提供网络安全性设备的组合，它还是安全策略的一个部分。安全策略建立了全方位的防御体系来保护机构的信息资源。安全策略告诉用户应有的责任、公司规定的网络访问、服务访问、本地和远程的用户认证、拨入和拨出、磁盘和数据加密、病毒防护措施和雇员培训等。所有可能受到网络攻击的地方都必须以同样的安全级别加以保护。仅设立防火墙系统，而没有全面的安全策略，那么防火墙就形同虚设。

引入防火墙的好处有：保护脆弱的服务；控制对系统的访问；集中的安全管理；增强的保密性；记录和统计网络利用数据以及非法使用数据；策略执行。

3. 防火墙的缺点

防火墙也有自身的限制，这些缺陷包括如下几个方面。

- 防火墙无法阻止绕过防火墙的攻击。因特网系统可能具有通过拨号连接到 ISP 去的功能。内部 LAN 可能提供一个调制解调器池，通过它就可以向外地的雇员或远程办公人员提供拨入服务，外部人员进而进入内部网络。
- 防火墙无法阻止来自内部的威胁，比如一个雇员无意间帮助外部入侵者的雇员造成的攻击。
- 防火墙无法防止病毒感染程序或文件的传输。因为在内部网中有各种操作系统和应用软件，所以要求防火墙扫描所有进来的文件、电子邮件和消息以确定是否有病毒，这不仅是不实用的，而且是不可能的。

12.3.2　防火墙的设计策略

防火墙通常有两种基本的设计策略：允许任何服务除非被明确禁止；禁止任何服务除非被明确允许。第一种的特点是“疑罪从无”，即“在被判有罪之前，任何嫌疑人都是无罪的”，它好用但不安全。第二种是“宁枉勿纵”，即“宁可错杀三千，也不放过一个”，它安全但不好用。在实际应用中防火墙通常采用第二种设计策略，但多数防火墙都会在两种策略之间采取折中的办法。

防火墙的设计策略包括网络策略和服务访问策略。影响防火墙系统设计、安装和使用的网络策略可分为两级，高级网络策略定义允许和禁止的服务以及如何使用服务，低级网络策略描述防火墙如何限制和过滤在高级策略中定义的服务。

服务访问策略主要包括因特网访问策略和外部网络来访策略（如拨入策略、SLIP/PPP 连接等）。服务访问策略必须是可行的和合理的。可行的策略必须在阻止已知的网络风险和提供用户服务之间取得平衡。典型的服务访问策略是允许已认证的用户在必要的情况下从因特网访问某些内部主机和服务；允许内部用户访问指定的因特网主机和服务。

【例 12-1】　网络在安装防火墙前拓扑结构如图 12-3 所示，具体环境如下。

① 外网（即外部网）接口 S1 地址为 202.112.169.6/30（子网掩码表示由 30 个 1 组成，下同），上联因特网接口地址为 202.112.169.5/30。

② 内网（即内部网）接口地址有两个。E0：202.112.168.2/28（可用地址空间是 202.112.168.1～202.112.169.14，广播地址为 202.112.168.15）。E0：192.168.1.1/24（内部网私有地址，地址空间为 192.168.1.1～192.168.1.254，广播地址为 192.168.1.255）。

③ 对外服务器默认网关为 202.112.168.1，内部主机默认网关地址为 192.168.1.1。

④ 内部网主机通过代理服务器上网。

要求使用防火墙，并制定相应策略来提高网络的安全性。

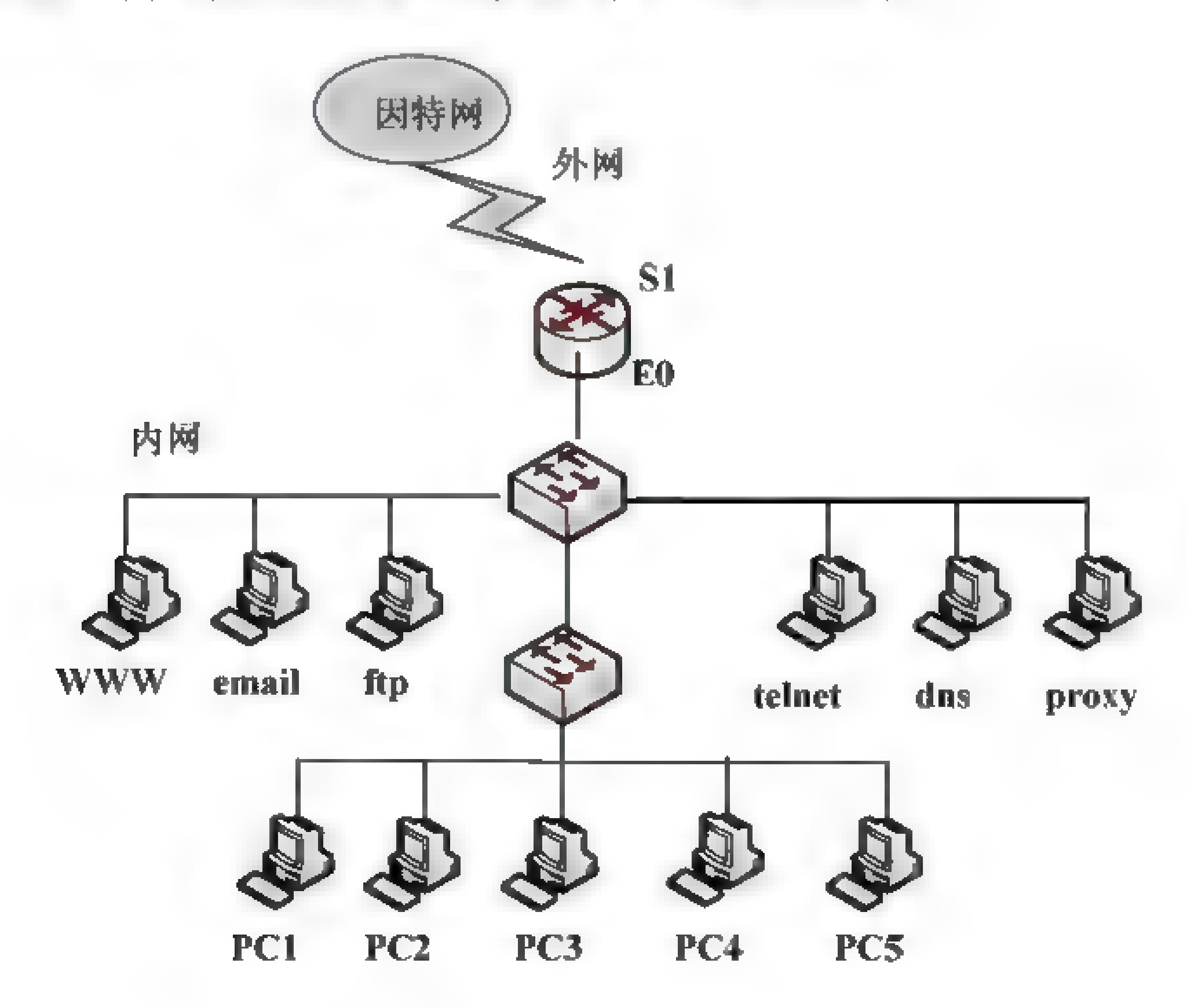


图 12-3　安装防火墙前网络拓扑结构

（1）防火墙部属

网络安装防火墙后，其拓扑结构如图 12-4 所示，具体环境如下。

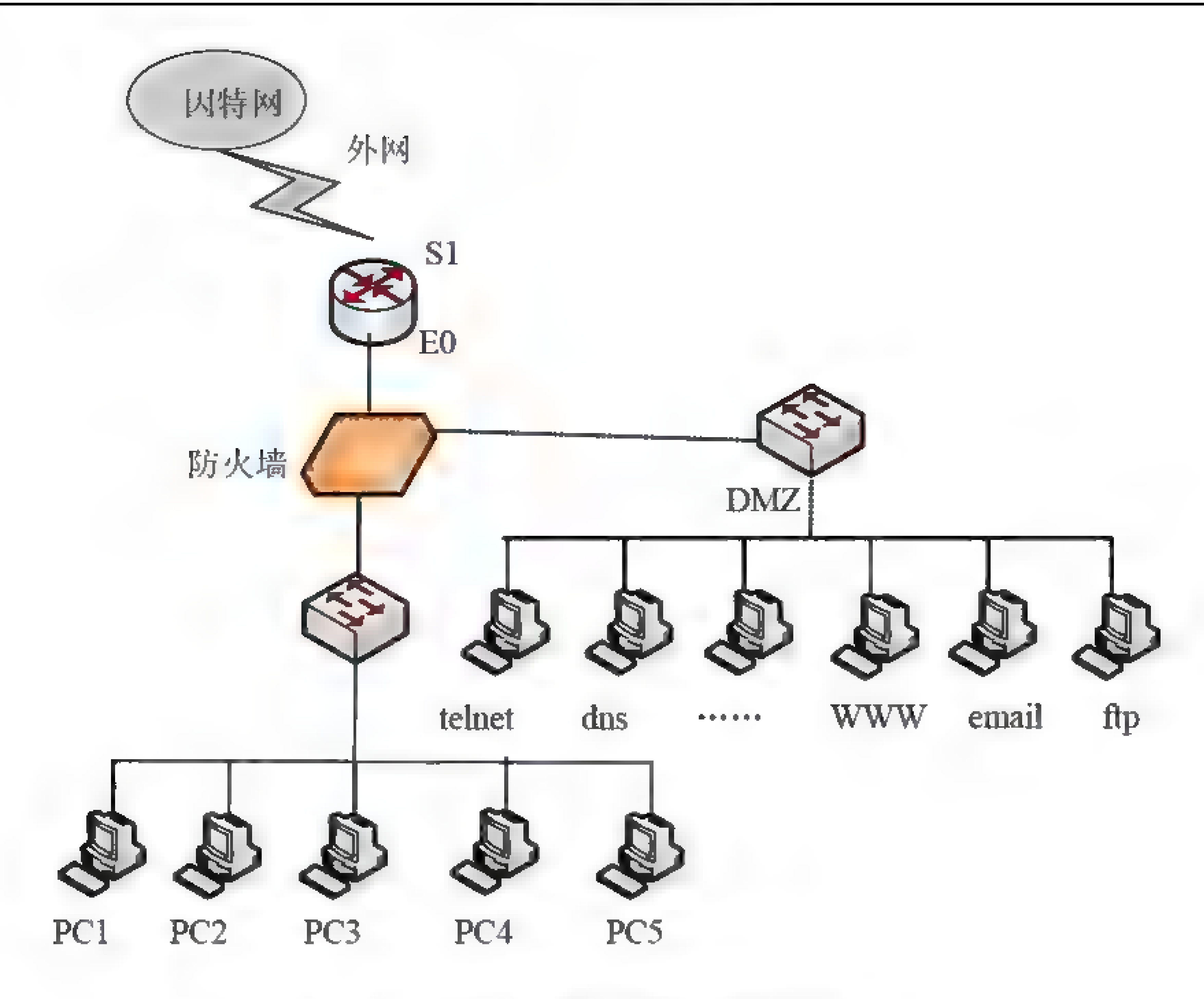


图 12-4 安装防火墙后网络拓扑结构

① 防火墙工作在混杂模式下。

② 内部主机同内部服务器系统严格分开。

③ 内部私有地址主机，内部服务器系统，外部网络分成严格的 3 个区域（内网、外围、DMZ 区域）。

④ 内网网口对应防火墙上接口 1，外网网口对应防火墙上接口 2，DMZ 区域对应防火墙接口 3。

⑤ 在各个区域之间实施严格的访问控制，保障系统安全。

⑥ 内部服务器系统采用公有地址，内部网访问外部网通过 NAT 实现，取代以前的代理服务器系统。

⑦ 将防火墙控制端放置在内部网。

⑧ 路由器上取消 E0 的第 2 个地址。

（2）配置策略

① 接口 1 设为防火墙的内部网接口和管理口，地址为 192.168.1.1，设置好相应的子网掩码后将其选为控制口。

② 将 DMZ 区域和外网区域设置为桥模式，同时在桥上绑定 IP 地址 202.112.169.6/28（为原来代理服务器地址）。

③ 添加内部网、DMZ 区域以及外部网个别设备。

④ 按照实际情况配置各种安全策略，如内部网访问 DMZ 区域各个服务器访问规则，根据不同服务配置不同的策略。

⑤ NAT 规则设置。在原系统中，内部网通过代理服务器上网。调整后，内部网的网络用户可以直接上网，不需要代理服务器。在防火墙上设置 NAT 功能实现地址转换。当内部网访问外部网络时，全部将内容地址转换为防火墙外部网地址。

12.4　计算机病毒

计算机病毒是指可以制造故障的一段计算机程序或一组计算机指令，它被计算机软件制造者有意无意地放进一个标准化的计算机程序或计算机操作系统中。然后，该病毒会依照指令不断地进行自我复制，也就是进行繁殖和扩散传播。

12.4.1　计算机病毒的特点

（1）非授权可执行性

用户执行一个程序时，把系统控制权交给这个程序，并分配给它相应的系统资源，如内存，从而使之能够运行以完成用户的需求，因此程序执行的过程对用户是透明的。而计算机病毒是非法程序，正常用户是不会明知是病毒程序，而故意调用执行。但由于计算机病毒具有正常程序的一切特性，可存储性和可执行性。它隐藏在合法的程序或数据中，当用户运行正常程序时，病毒伺机窃取到系统的控制权，抢先运行，然而此时用户还认为在执行正常程序。

（2）隐蔽性

计算机病毒是一种编程技巧很高、短小精悍的可执行程序。它通常黏附在正常程序之中或磁盘引导扇区中，或者磁盘上标为坏簇的扇区中，以及一些空闲概率较大的扇区中，这是它的非法可存储性。病毒想方设法隐藏自身，就是为了防止用户察觉。

（3）传染性

传染性是计算机病毒最重要的特征，是判断一段程序是否为计算机病毒的依据。病毒程序一旦侵入计算机系统就开始搜索可以传染的程序或者磁介质，然后通过自我复制迅速传播。由于目前计算机网络日益发达，计算机病毒可以在极短的时间内，通过像因特网这样的网络传播世界。

（4）潜伏性

计算机病毒具有依附于其他媒体而寄生的能力，这种媒体称之为计算机病毒的宿主。依靠病毒的寄生能力，病毒传染合法的程序和系统后，不立即发作，而是悄悄地隐藏起来，然后在用户不察觉的情况下进行传染。这样，病毒的潜伏性越好，它在系统中存在的时间也就越长，传染的范围也越广，危害性也越大。

（5）破坏性

无论何种病毒程序一旦侵入系统都会对操作系统的运行造成不同程度的影响，即使不直接产生破坏作用的病毒程序也要占用系统资源（如占用内存空间，占用磁盘存储空间以及系统运行时间等）。而绝大多数病毒程序要显示一些文字或图像，影响系统的正常运行，还有一些病毒程序删除文件，加密磁盘中的数据，甚至摧毁整个系统和数据，使之无法恢复，造成无可挽回的损失。因此，病毒程序的副作用轻者降低系统工作效率，重者导致系统崩溃、数据丢失。病毒程序的表现性或破坏性体现了病毒设计者的真正意图。

（6）可触发性

计算机病毒一般都有一个或者几个触发条件。满足其触发条件时要么激活病毒的传染机制，使之进行传染；要么进行传染；要么激活病毒的表现部分或破坏部分。触发的实质是一种条件的控制，病毒程序可以依据设计者的要求，在一定条件下实施攻击。这个条件

可以是敲入特定字符，使用特定文件，等待某个特定日期或特定时刻，或者是病毒内置的计数器打到一定次数等。

12.4.2 计算机病毒的分类

从第一个病毒出世以来，病毒的数量仍在不断增加。据统计，计算机病毒以每周 10 种的速度递增。下面对计算机病毒种类进行分类，以便更好地了解病毒。

1. 按传染方式分类

计算机病毒按传染方式分为引导型病毒、文件型病毒和复合型病毒。以下分别对三种类型做出介绍。

（1）引导型病毒

引导型病毒是指寄生在磁盘引导区或主引导区的计算机病毒。此种病毒利用系统引导时不对主引导区内容的正确性进行判别的缺点，在引导系统的过程中侵入系统，驻留内存，监视系统运行，伺机传染和破坏。按照引导型病毒在硬盘上的寄生位置又可细分为主引导记录病毒和分区引导记录病毒。主引导记录病毒感染硬盘的主引导区，如大麻病毒、2708 病毒和火炬病毒等；分区引导记录病毒感染硬盘的活动分区引导记录，如小球病毒、Girl 病毒等。

（2）文件型病毒

文件型病毒是指能够寄生在文件中的计算机病毒。这类病毒程序感染可执行文件，如 1575/1591 病毒、848 病毒感染.COM 和.EXE 等可执行文件，Macro/Concept、Marco/Atoms 等宏病毒感染.DOC 文件。

（3）复合型病毒

复合型病毒具有引导型病毒和文件型病毒的寄生方式。这种病毒扩大了病毒程序的传染途径，既感染磁盘的引导记录，又感染可执行文件。当染有此种病毒的磁盘用于引导系统或调用执行染毒文件时，病毒都会被激活。因此在检测、清除复合型病毒时，必须全面彻底地根治此种病毒。如果只被该病毒的一个特性，把它只当作引导型或文件型病毒进行清除的话，虽然好像是清除了，但还留有隐患，并且这种经过消毒后的“洁净”系统更赋有攻击性。这种病毒有 Flip 病毒、新世纪病毒和 One-half 病毒等。

2. 按连接方式分类

计算机病毒按连接方式可分为源码型病毒、入侵型病毒、操作系统型病毒和外壳型病毒，以下分别对其进行介绍。

（1）源码型病毒

源码型病毒较为少见，并且很难编写。因为它要攻击高级语言编写的源程序，在源程序编译之前插入其中，并且随源程序一起编译、链接成可执行文件。此时刚刚生成的可执行文件便已经感染了病毒。

（2）入侵型病毒

入侵型病毒可用自身代替正常程序中的部分模块或堆栈区。因此这类病毒只攻击某些特定程序，针对性强，一般情况下难以被发现，清除起来也比较困难。

（3）操作系统型病毒

操作系统型病毒可用自身部分加入或替代操作系统的部分功能。因其直接感染操作系统，这类病毒的危害性较大。

（4）外壳型病毒

外壳型病毒将自身附在正常程序的开头或结尾，相当于给程序加了个外壳。大部分的文件型病毒都属于这一类。

3. 按破坏性分类

计算机病毒按破坏性分为良性病毒和恶性病毒。以下分别对其做出介绍。

（1）良性病毒

良性病毒是指那些只为了表现自身，并不彻底破坏系统和数据，但会大量占用 CPU 时间，增加系统开销，降低系统工作效率的一类计算机病毒。这种病毒多数是恶作剧者的产物，他们的目的不是为了破坏系统和数据，而是为了让使用染有病毒的计算机用户通过显示器或扬声器看到或听到病毒设计者的编程技术。这类病毒有小球病毒、1575/1591 病毒、救护车病毒、扬基病毒和 Dabi 病毒等。还有一些人利用病毒的这些特点宣传自己的政治观点和主张。也有一些病毒设计者在其编制的病毒发作时进行人身攻击。

（2）恶性病毒

恶性病毒是指那些一旦发作后，就会破坏系统或数据，造成计算机系统瘫痪的一类计算机病毒。这类病毒有黑色星期五病毒、火炬病毒和米开朗基罗病毒等。这种病毒危害性极大，有些病毒发作后可以给用户造成不可挽回的损失。

12.4.3　计算机病毒的防治

（1）病毒的防治策略

病毒防治的根本目的是保护用户的数据安全，因此病毒的防治策略可以从以下三个方面入手：数据备份、封堵漏洞，查杀病毒和灾难恢复。

数据备份是降低病毒破坏性的最有效方法。经常进行数据备份，即使遭到病毒攻击，也不至于丢失关键数据。对付病毒，一方面封堵系统及应用程序漏洞，另一方面还要积极地、经常地查杀病毒。同时对于一些灾难性的或不可避免的损失，使用灾难恢复同样是一个重要的防毒措施。用户系统发身故意外、数据遭受损失破坏后，应立即关闭系统，以防止更多的数据遭受破坏，然后根据具体情况选择合适的方案进行数据恢复。

（2）病毒的防治和查杀方法

对用户而言，降低病毒破坏程度的最佳策略是防患于未然，即采取有效措施，尽最大可能地防止计算机感染病毒。由于病毒大多是利用系统或应用程序的漏洞进行攻击和破坏的，因此封堵漏洞可以减少遭受病毒攻击的几率，封堵漏洞要从 3 个方面着手。

- 要对网络和每台计算机正确配置，特别要注意安全权限等关键配置，防止因配置疏忽留下漏洞而给病毒可乘之机。
- 尽量不安装或者关闭不需要或不安全的功能性应用程序。
- 要经常从相关的网站下载补丁程序，及时完善系统和应用程序，尽量减少系统和应用程序漏洞。

封堵漏洞、查杀病毒是对抗病毒最有效的手段。网络环境下，病毒的查杀方法较多，它们各有其优缺点。

12.5　网络攻击与防范

涉及网络安全的问题很多，最重要的问题就是人为的网络攻击，尤其是在因特网互联全球的过程中，网络攻击更是比比皆是。本节将针对常见的网络攻击和防范措施做详细介绍。

12.5.1　网络攻击方法分析

当信息从信源向信宿流动时，可能会受到各种类型的攻击，如图 12-5 所示。

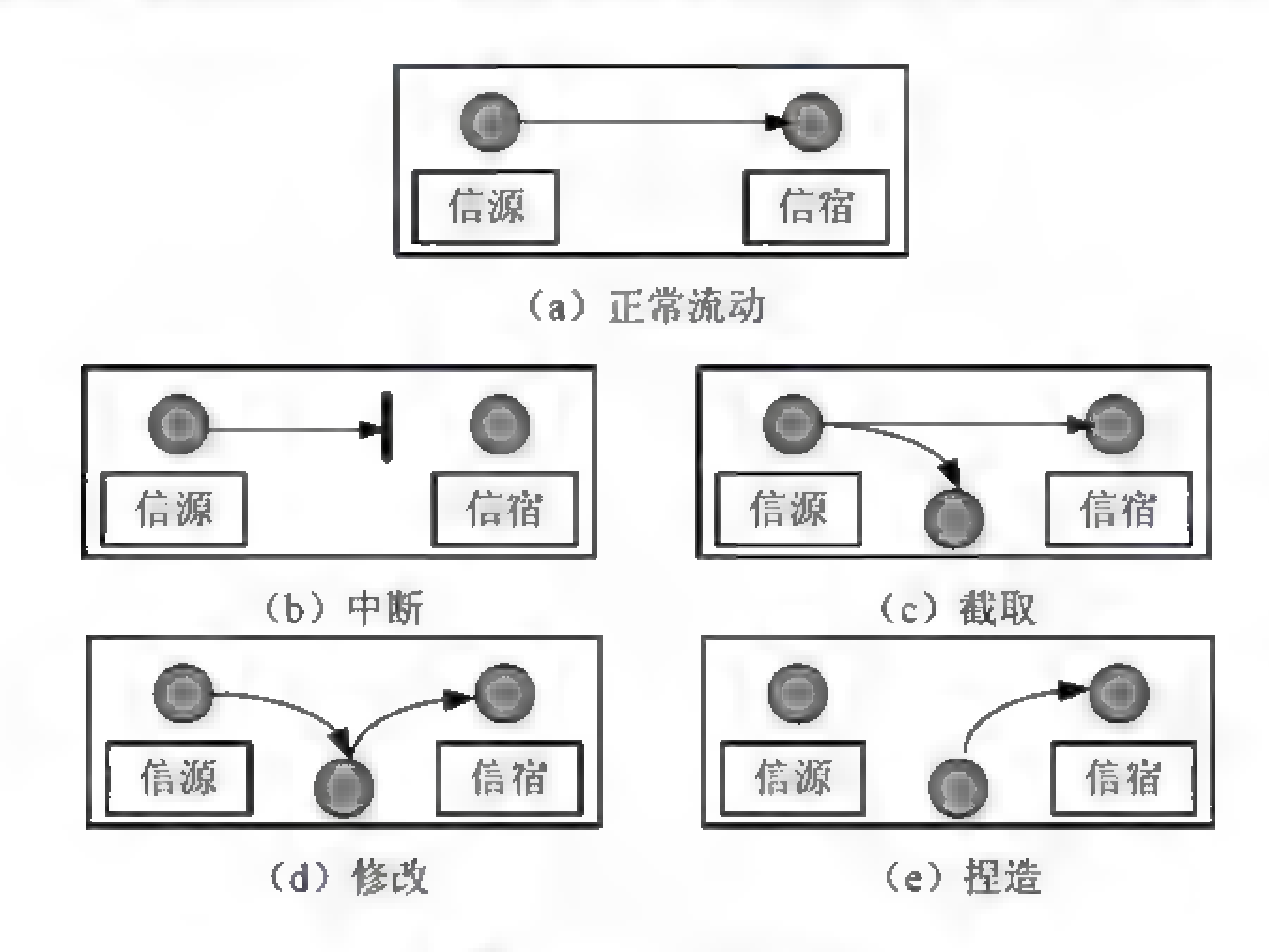


图 12-5　安全攻击

① 中断是指系统资源遭到破坏或变得不能使用。这是对可用性的攻击。例如，对一些硬件进行破坏、切断通信线路或禁用文件管理系统。

② 截取是指未授权的实体得到了资源的访问权。这是对机密性的攻击。未授权实体可能是一个人、一个程序或一台计算机。例如，为了捕获网络数据的窃听行为，以及在未授权的情况下复制文件或程序的行为。

③ 修改是指未授权的实体不仅得到了访问权，而且还篡改了资源。这是对完整性的攻击。例如，在数据文件中改变数值、改动程序使它按不同的方式运行和修改在网络中传送的消息的内容等。

④ 捏造是指未授权的实体向系统中插入伪造的对象。这是对合法性的攻击。例如，向网络中插入欺骗性的消息；或者向文件中插入额外的记录。

1. 被动攻击和主动攻击

安全攻击可分为被动攻击和主动攻击两种，如图 12-6 所示。

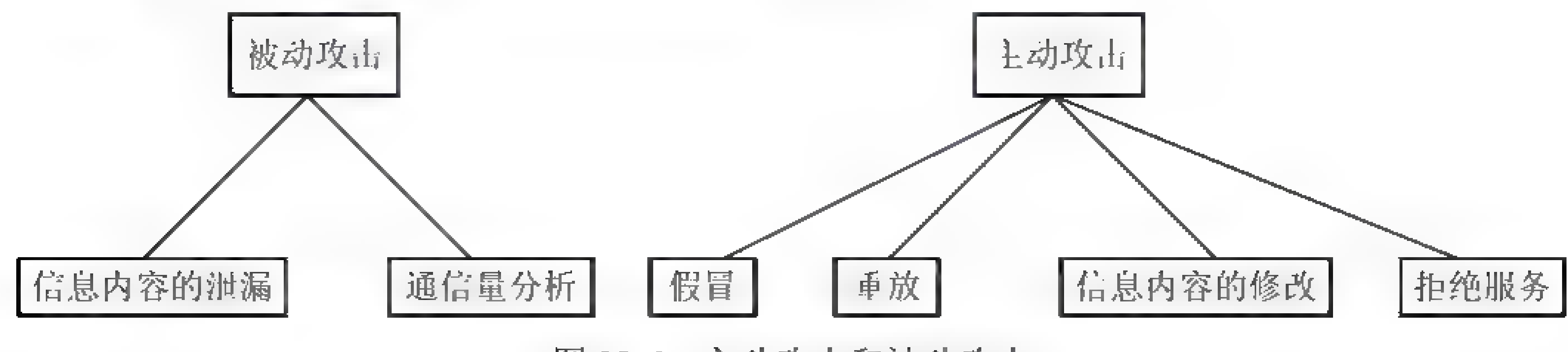


图 12-6　主动攻击和被动攻击

被动攻击的特点是偷听或监视传送。其目的是获得正在传送的信息。被动攻击有泄露信息内容和通信量分析等。

泄露信息内容容易理解。电话对话、电子邮件消息、传递的文件中可能含有敏感的机密信息。我们要防止对手从传送中获得这些内容。

主动攻击涉及修改数据流或创建数据流，它包括假冒、重放、修改消息和拒绝服务等。

① 假冒是一个实体假装成另一个实体。假冒攻击通常包括一种其他形式的主动攻击。例如，在发送身份验证序列时，可以捕获身份验证序列并重新执行，这样，通过扮演具有特权的实体，使几乎没有特权的实体获得了额外的特权。

② 重放涉及被动捕获数据单元及其后来的重新传送，以产生未经授权的效果。

③ 修改消息意味着改变了真实消息的部分内容，或将消息延迟或重新排序，导致未授权的操作。

④ 拒绝服务是指禁止通信实体的正常使用或管理。这种攻击拥有特定的目标，例如，实体可以取消送往特定目的地址的所有消息（例如安全审核服务）。另一种拒绝服务的形式是整个网络的中断，这可以通过使网络失效而实现，或通过消息过载使网络性能降低。

主动攻击具有与被动攻击相反的特点。虽然很难检测出被动攻击，但可以采取措施防止它的成功。相反，很难绝对预防主动攻击，因为这样需要在任何时候对所有的通信工具和路径进行完全的保护。防止主动攻击的做法是对攻击进行检测，并从它引起的中断或延迟中恢复过来。因为检测具有威慑的效果，它也可以对预防做出贡献。

2. 服务攻击和非服务攻击

从网络高层协议的角度划分，攻击方法可以概括地分为两大类：服务攻击与非服务攻击。服务攻击是针对某种特定网络服务的攻击，如针对 E-mail 服务、Telnet、FTP 和 HTTP 等服务的专门攻击，例如 Telnet 服务在 23 端口上提供远端连接，HTTP 在 80 端口等待客户的 WWW 浏览请求等情况是众所周知的。目前因特网的 TCP/IP 协议缺乏认证、保密措施，是造成服务攻击的重要原因。现在有很多具体的攻击工具，如 Mail Bomb（邮件炸弹）等，可以很容易的实施对某项服务的攻击。

非服务攻击不针对某项具体应用服务，而是基于网络层等低层协议而进行的 TCP/IP 协议（尤其是 IP v4）自身的安全机制不足为攻击者提供了方便之门，如源路由攻击和地址欺骗都属于这一类。现在有很多现成的软件可以实施非服务攻击，如 NetXRay 等。

与服务攻击相比，非服务攻击与特定服务无关，往往利用协议作系统实现协议时的漏洞来达到攻击的目的，更为隐蔽，而且目前也是常常被忽略的方面，因而被认为是一种更为有效的攻击手段。

12.5.2　入侵检测的基本概念

入侵检测（Intrusion Detection，ID），顾名思义，是对入侵行为的发觉。它通过对计算机网络或计算机系统中的若干关键点收集信息并对其进行分析，从中发现网络或系统中是否有违反安全策略的行为和被攻击的迹象。进行入侵检测的软件与硬件的组合便是入侵检测系统（Intrusion Detection System，IDS）。与其他安全产品不同的是，入侵检测系统需要更多的智能，必须可以将得到的数据进行分析，并得出有用的结果。一个合格的入侵检测系统能大大简化管理员的工作，保证网络安全地进行。

入侵检测是对防火墙及其有益的补充，能够帮助网络系统快速发现网络攻击的发生，

扩展了系统管理员的安全管理能力（包括安全审计、监视、进攻识别和响应），提高了信息安全基础结构的完整性。入侵检测被认为是防火墙之后的第二道安全闸门，在不影响网络性能的情况下能对网络进行监听，从而提供对内部攻击、外部攻击和误操作的实时保护。

在本质上，入侵检测系统是一个典型的“窥探设备”。它不跨接多个物理网段，无须转发任何流量，而只需要在网络上被动的、无声息的收集它所关心的报文即可。对收集来的报文，入侵检测系统提取相应的流量统计特征值，并利用内置的入侵知识库，与这些流量特征进行智能分析比较匹配。根据预设的阀值，匹配耦合度较高的报文流量将被认为是攻击，入侵检测系统将根据相应的配置进行报警或进行有限度的反击。

1. IDS 功能与模型

一个合格的入侵检测系统能大大简化管理员的工作，保证网络安全地进行。具体说来，入侵检测系统的主要功能有以下几点。

- 检测并分析用户和系统的活动。
- 核查系统配置和漏洞。
- 评估系统关键资源和数据文件的完整性。
- 识别已知的攻击行为。
- 统计分析异常行为。
- 操作系统日志管理，并识别违反安全策略的用户活动。

最早的入侵检测模型由 Dorothy Denning 在 1987 年提出。这个模型与具体系统和具体输入无关，并对此后的大部分实用系统都有很高的借鉴价值。图 12-7 给出了这个通用模型的体系结构。事件产生器可根据具体应用环境而有所不同，一般可来自审计记录、网络数据包以及其他可视行为。这些事件构成了检测的基础。行为特征表是整个检测系统的核心，包含了用于计算用户行为特征的所有变量。这些变量可根据具体所采纳的统计方法及事件记录中的具体动作模式而定义，并根据匹配记录数据更新变量值。

如果统计变量的值达到了异常程度，则行为特征表产生异常记录，并采取一定的措施。规则模块可以由系统安全策略、攻击模式等组成。它一方面以判断是否被攻击提供参考机制，另一方面根据事件记录、异常记录以及有效日期等控制并更新其他模块的状态。在具体实现上，规则的选择与更新的可能不尽相同，但通常，行为特征模块执行基于行为的检测，而规则模块执行基于知识的检测。

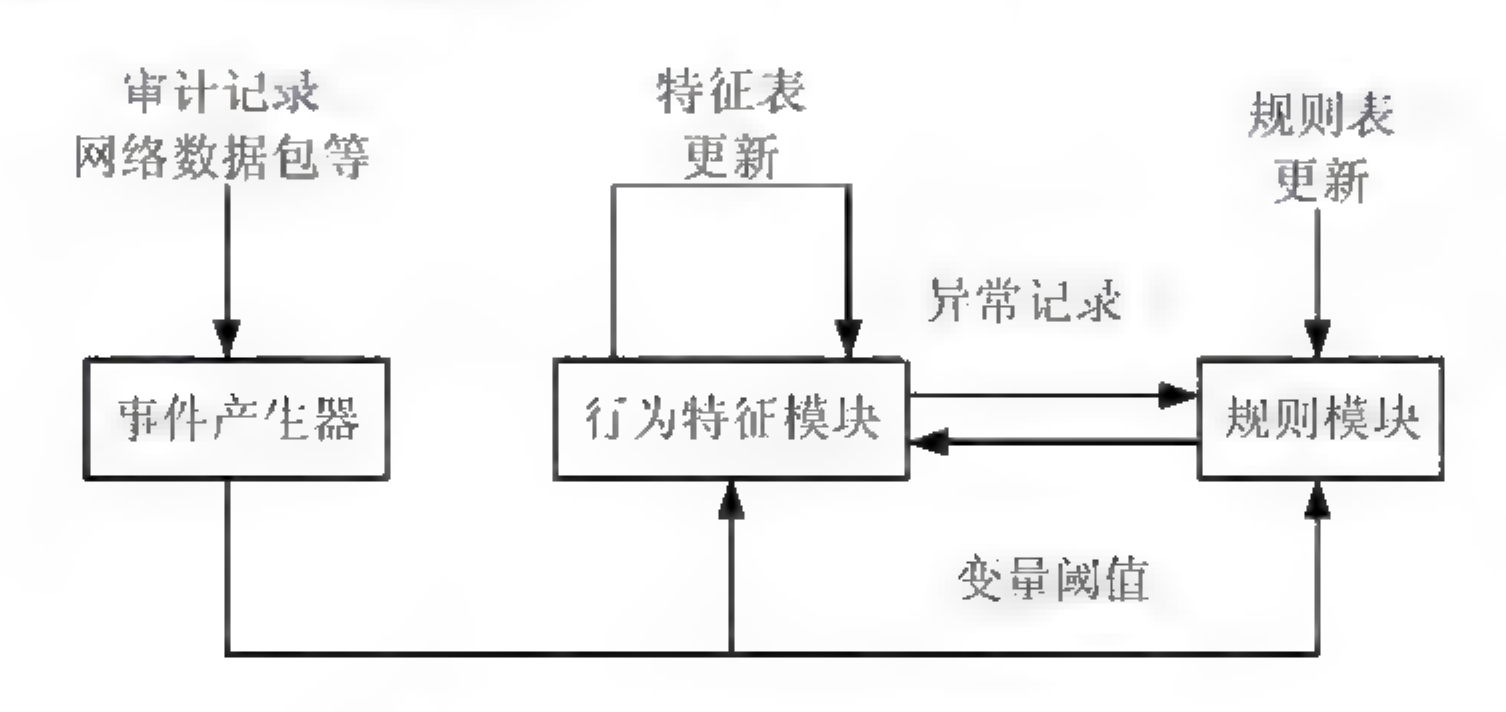


图 12-7 通用的入侵检测模型

2. IDS 系统结构

入侵检测是监测计算机网络和系统以发现违反安全策略事件的过程。通常，入侵检测

系统由以下三个功能部件组成。

- 事件发生器——提供事件记录流的信息源。
- 分析引擎——接收来自信息源的数据并检查数据以发现入侵迹象。
- 响应部件——对基于分析引擎的结果产生反应。

入侵检测源于传统系统审计的实现。当审计作为保护敏感系统的方法被提出时，确保审计信息的可信就成为很自然的事。在一个环境中，审计信息必须与它要保护的系统分开来存储和处理。大多数入侵检测方法都继承了这个要求，将审计信息和它要保护的系统分隔开来，这是因为要防止入侵者通过删除审计记录来使入侵检测系统失效；要防止入侵者通过修改入侵监测器的结果来隐藏入侵的存在；要减轻操作系统执行入侵检测任务带来的操作负载；在这种体系结构中，运行入侵检测系统的系统叫做主机，被检测的系统或网络叫做目标机。

3. 监测策略

入侵检测的第一要素是数据源。数据源可以以多种方式进行分类。以数据存在的位置来对数据进行分类，数据源可分为 4 类，来自主机的数据、来自网络的数据、来自应用程序的和来自目标机的数据。根据以上 4 类数据源，就有 4 种不同的监测策略。

- 基于主机的监测：收集通常在操作系统层，来自计算机内部的数据。
- 基于网络的监测：收集网络数据包。
- 基于应用程序的监测：收集来自运行应用程序的数据。
- 基于目标机的监测：产生自己的数据。

4. IDS 类型

入侵检测系统有不同的分类标准，按照信息源划分入侵检测系统是目前最通用的划分方法。入侵检测系统分为四类，即基于主机的 IDS、基于网络的 IDS、基于目标的 IDS 和基于应用的 IDS。基于网络的 IDS 和基于主机的 IDS 是目前最常用的两类 IDS，下面主要对这两类 IDS 进行分析。

（1）基于网络的 IDS

基于网络的入侵检测使用原始的数据包作为数据源。通常将主机的网卡设成混杂模式（promiscuous mode），实时监视并分析通过网络的所有通信业务。基于网络的入侵检测系统担负着保护整个网段的任务，它的攻击识别模块通常使用 4 种技术来识别攻击标识。

- 模式、表达或字节匹配。
- 频率或穿越阈值。
- 次要事件的相关性。
- 统计学意义上的非常规则现象检测。

一旦检测到了攻击行为，入侵检测系统的响应模块就会对攻击采取相应的反应。反应因产品而异，但通常都包括通知管理员、中断连接、为法庭分析和证据收集而做的会话记录。

基于网络的入侵检测系统能完成许多基于主机的入侵检测系统无法提供的功能。实际上，许多客户在最初使用入侵检测系统时，都配置了基于网络的入侵检测，因为它具有成本低、反应速度较快等优点。

（2）基于主机的 IDS

基于主机的入侵检测往往以系统日志、应用程序日志等作为数据源，当然也可以通过其他手段从所在的主机收集信息进行分析。基于主机的入侵检测系统保护的一般是所在的系统。

基于主机的 IDS 分析的信息来自于单个的计算机系统，这使得它能够相对可靠、精确地分析入侵活动，能精确地决定哪一个进程和用户参与了对操作系统的一次攻击。此外，不像基于网络的 IDS，基于主机的 IDS 能“看到”一次企图攻击的结局，因为它能直接控制和监视那些攻击者感兴趣的数据文件和系统进程。

尽管基于主机的入侵检测系统不如基于网络的入侵检测系统快捷，但它确实具有基于网络的入侵检测系统无法比拟的优点。这些优点包括更好的辨识分析、对特殊主机事件的紧密关注及低廉的成本。

12.5.3 发展方向

无论从规模与方法上，入侵技术近年来都发生了变化。入侵的手段与技术也有了“进步与发展”。入侵技术的发展与演化主要反映在下列几个方面。

（1）入侵或动机的综合化与复杂化

入侵的手段有多种，入侵者往往采取多种攻击手段。由于网络防范技术的多重化，攻击的难度增加，使得入侵者在实施入侵或攻击时往往同时采取多种入侵的手段，以保证入侵的成功概率，并可在攻击实施的初期掩盖攻击或入侵的真实目的。

（2）入侵主体对象的间接化，即实施入侵与攻击的主体的隐蔽化

通过一定的技术，可掩盖主体的源地址及主机地址。即使用了隐蔽技术后，对于被攻击对象的攻击主体是无法直接确定的。

（3）入侵或攻击的规模扩大

对于网络的入侵与攻击，其初期往往是针对某公司或一个网站，其攻击的目的可能是某些网络技术爱好者的猎奇行为，也不排除商业的盗窃与破坏行为。由于战争对电子技术与网络技术的依赖性越来越大，随之产生、发展、逐步升级到电子战与信息战。信息战无论其规模与技术都与一般意义上的计算机网络的入侵与攻击不可相提并论。信息战的成败关系到国家主干通信网络的安全，是与任何主权国家领土安全一样重要的国家安全。

（4）入侵或攻击的分布化

以往常用的入侵与攻击行为往往由单机执行，由于防范技术的发展使得此类行为不能奏效。所谓的分布式拒绝服务（DDoS）在很短时间内可造成被攻击主机的瘫痪。且此类分布式的单击信息模式与正常通信无差异，所以往往在攻击发动的初期不易被确认。分布式攻击是近期最常用的攻击手段。

（5）攻击对象的转移

入侵与攻击常以网络为侵犯的主体，但近期来的攻击行为却发生了策略性的改变，由攻击网络改为攻击网络的防护系统，且有愈演愈烈的趋势。现已有专门针对 IDS 作攻击的报道。攻击者详细地分析了 IDS 的审计方式、特征描述、通信模式等，找出 IDS 的弱点，然后加以攻击。

目前看来，入侵检测技术大致朝下述三个方向发展。

① 分布式入侵检测

第一层含义即针对分布式网络攻击的检测方法；第二层含义即使用户分布式的方法

来检测分布式的攻击，其中的关键技术是检测信息的协同处理与入侵攻击的全局信息的提取。

② 智能化入侵检测

使用智能化的方法与手段来进行入侵检测。所谓的智能化方法，现阶段常用的精神网络、遗传算法、模糊技术和免疫原理等方法，常用于入侵特征的辨识与泛化。利用专家系统的思想来构建入侵检测系统也是常用的方法之一，特别是具有自学能力的专家系统，实现了知识库的不断更新与扩展，使设计的入侵检测系统的防范能力不断增强，具有更广泛的应用前景。应用智能体的概念来进行入侵检测的尝试也已有报道。较为一致的解决方案是高效常规意义下的入侵检测系统与具有智能检测功能的检测软件或模块的结合使用。

③ 全面的安全防御方案

使用安全工程风险管理的思想与方法来处理网络安全问题，讲网络安全作为一个整体工程来处理，从管理、网络结构、加密通道、防火墙、病毒防护和入侵检测多方位全面对所关注的网络作全面的评估，然后提出可行的全面解决方案。

【例 12-2】 网络在部属入侵检测系统前拓扑结构如图 12-8 所示，如果要在该网络中部属网络 IDS 和主机 IDS，应该如何部属，各有什么优缺点。

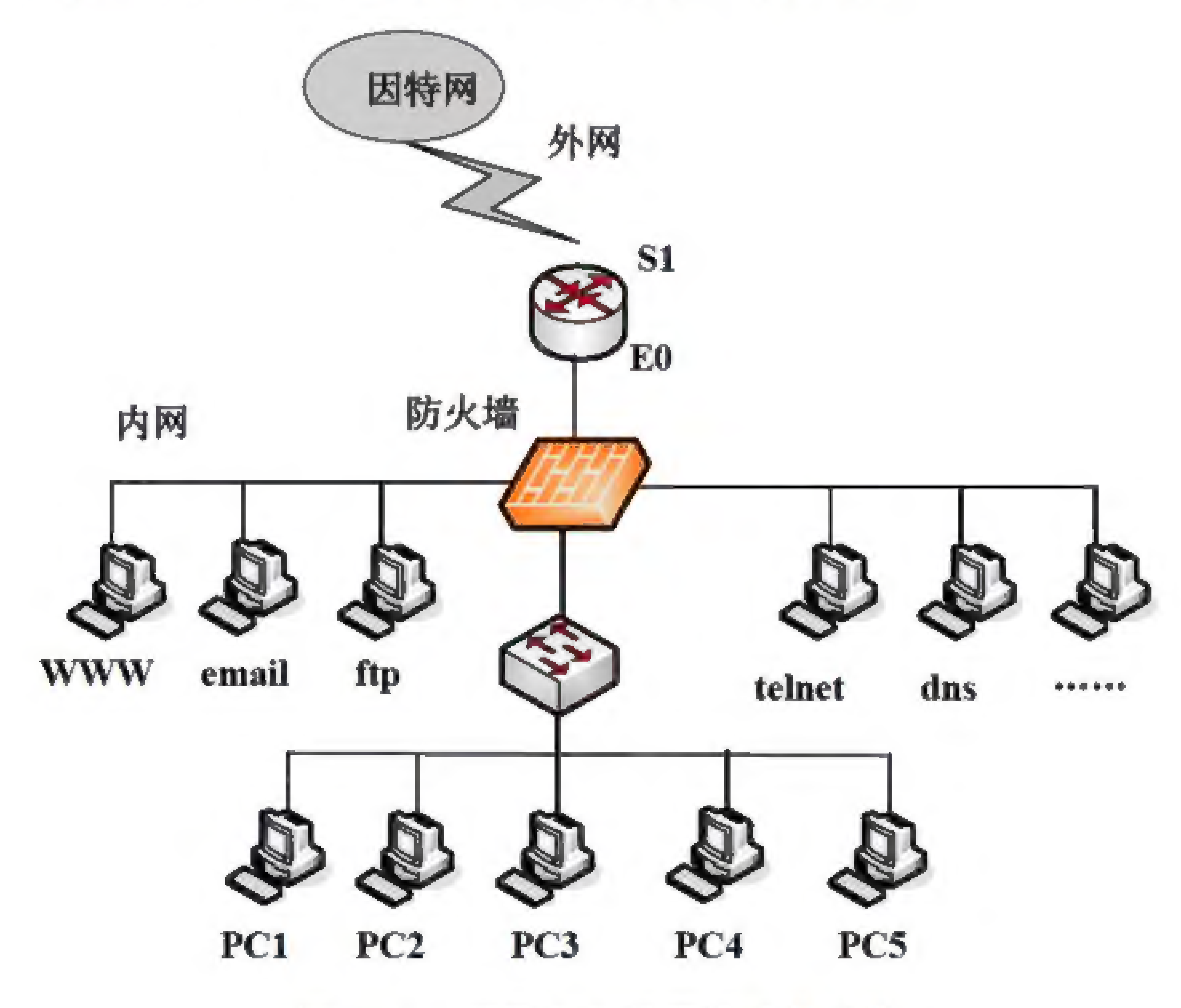


图 12-8　部属 IDS 前网络拓扑结构

（1）使用网络 IDS

网络 IDS 的名称来自于它的工作模式——监视整个网络。更精确地说，它监视整个网络的一部分。部属网络 IDS 后的拓扑结构如图 12-9 所示，我们使用了 3 个 NIDS，这些 IDS 都被放置在网络最关键的地方，能监视到关键部位处所有设备的网络流量。这是一个典型的网络保护方案拓扑图，提供公共服务器子网被 NIDS 保护着，子网中的一台服务器被入侵后，这台服务器便称为一个继续攻击整个子网的跳板。为了预防更深层次的危险，必须监视这个子网。

内网中的主机被其他的网络 IDS 保护着，这样可以减少内网主机被入侵的危险，在网络中部属多个 NIDS 时深层安全防护的典型。

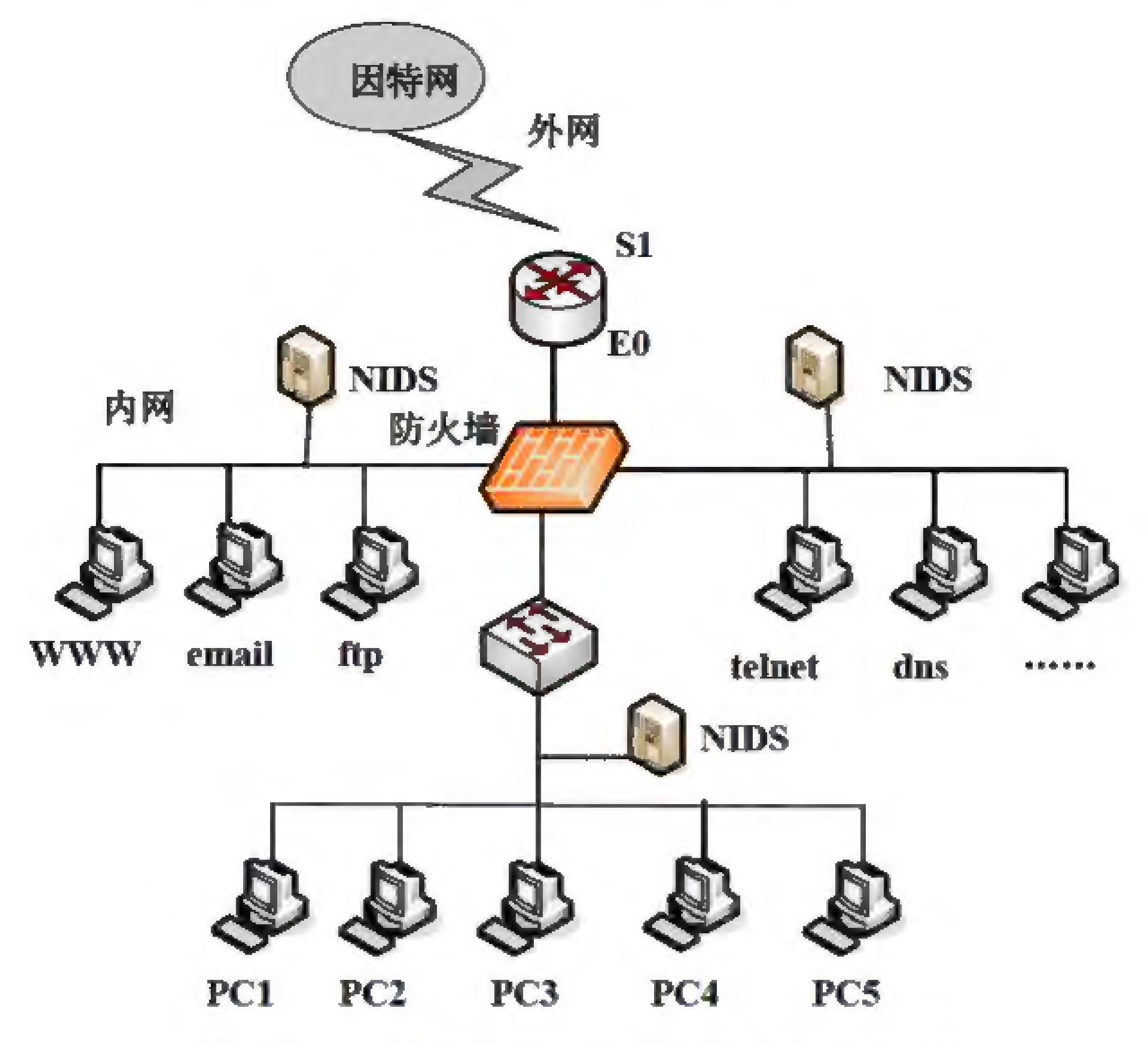


图 12-9　部属网络 IDS 后网络拓扑结构

（2）使用主机 IDS

主机 IDS 和网络 IDS 有所不同，它只能保护所在的计算机。它的一个好处是可以精确地根据自己的需要制定规则。例如，如果运行 HIDS 的计算机上没有运行域名服务（DNS），就不需要添加那些检测 DNS 攻击地规则集，减少了不相关的规则，可以提高检测效率和降低机器负荷。

图 12-10 的拓扑图是一个在服务器和个人计算机上安装了 HIDS 的网络。正如前面所说的，安装在邮件服务器上的 HIDS 主要只设置和邮件服务器相关的规则，使其免受入侵；而安装在 WWW 服务器上的 IDS 主要设置和 Web 服务相关的规则，检测对 WWW 服务器的攻击。在安装时，零散的个人计算机可以使用常用的规则集，当有新的漏洞公布后，规则要及时和定期地更新以检测新漏洞。

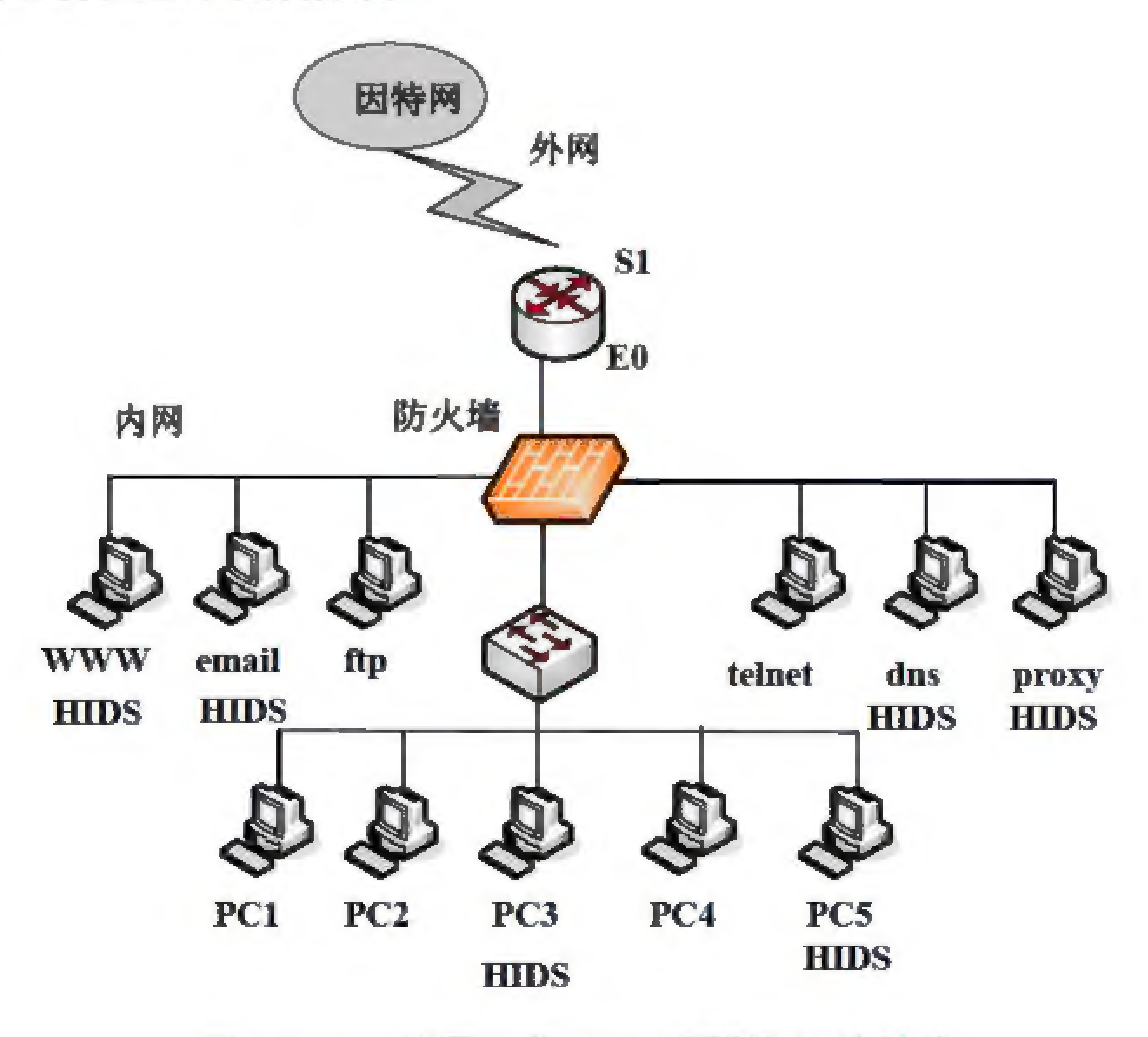


图 12-10　部属主机 IDS 后网络拓扑结构

习题

1. 描述计算机网络安全的组成及影响网络安全的因素。
2. 列举你所知道的操作系统所达到的可信计算机系统评估标准。
3. 对网络安全的威胁有哪些？有哪些安全策略？
4. 对称加密体制与公钥体制各有什么特点以及有何优缺点？
5. 简单描述 DES 的加密过程。
6. 简单描述数字签名的原理。
7. 描述常见的网络攻击。
8. 描述防火墙的工作原理和所提供的功能。
9. 描述入侵检测的工作原理和特点。
10. 列举 1 个常见的入侵检测系统，并说明其工作特点。